`

Department of Information Technology

POLICIES AND PROCEDURES

MANUAL 2013

Table of Contents

Policy 01: Customer Support

Policy Statement

The Information Technology resources and services of Prince Mohammed Bin Fahd University are provided for the advancement of the University's educational, research, and service objectives. They are offered primarily to facilitate the University's academic and business purposes.

University Service Desk

To ensure support for all students, faculty and staff members, ITD has established a customer service desk commonly known as helpdesk. In order to help our customers, ITD provides a service desk (Helpdesk) software package to track and trace all IT and facilities issues to successful resolution and ensure customer satisfaction. Requests for the provisioning of new services are also handled by service desk.

IT Equipment Refresh

Personal computers in labs and classrooms, as well as faculty computers, are on a 3-5 year replacement cycle.

Applicability

IT Policies are applicable to all students and employees (faculty, administrators,

and staff) and any others who are extended the privilege of using IT resources and services for the purpose of achieving the educational objectives of PMU and its students. All such persons accessing and using IT resources and services are subject to the applicable provisions of the University Statutes, University Code of Conduct, and Handbook for Administrators, Student Handbooks, and all other policies and procedures established by administrative offices of PMU.

Policy 02: Acceptable Use

Policy Statement

The following Executive Policy Statements govern the Responsibilities for Users Functional Policies listed in this document:

- All relevant statutory, regulatory and contractual requirements must be explicitly defined by the HR Department and technical requirements must be explicitly defined and documented by PMU for each information system.
- Appropriate procedures must be implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights and on the use of proprietary software products;
- Important records of PMU must be protected from loss, destruction and falsification;
- Controls must be applied to protect staff personal information in accordance with relevant legislation;
- Management must authorize the use of information processing facilities and controls must be applied to prevent the misuse of such facilities;
- Controls must be in place to ensure compliance of Information systems with national agreements, laws, regulations or other instruments to control the access to or use of cryptographic controls. This must be regularly reviewed;
- Where action against a person or organisation involves the law, either civil or criminal, the evidence presented must conform to the rules for evidence laid down in the relevant law;
- This must include compliance with any published functional policy or code of practice for the production of admissible evidence.

.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.
Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets (Digital Media)
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as network link
- All management information systems
- All business activities supported by ITD Group.
- All of the above are either owned or leased by the ITD Group and under the PMU-ITD possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Use of the Internet/Intranet – Internet Crime

Current Legislation

The Saudi Arabian Communications and Information Technology Commission announced the issuance of e-crimes and e-transaction acts, Both acts were issued on 27'th of March, 2007. E-crimes act was issued to combat information electronic crimes, by defining those crimes and penalties upon them. E-transactions act was issued to regulate electronic transactions and electronic signatures in a policy frame work, and combat any misuse of them by defining responsibilities, and penalties.

University Directive

All users must comply with the following functional policies:

Internet/Intranet Functional Policy

Hacking and Cracking into Computer systems

- No employees will participate or be party to any kinds of hacking or cracking into computer systems.
- No user is allowed to gain access to PMU computer networks and systems without prior permission from the designated authority within PMU.
- No vendor or third party is permitted to perform penetration testing on any of PMU systems and network without written approval from PMU.
- All users are allowed to perform only authorized transactions on PMU systems and the Internet/Intranet.

Creating and distribution of malicious (dangerous) code

Dangerous code can be classified as any computer program (code) that causes destruction or harm to a computer system.

- All users must ensure they have Anti-virus software enabled on their computers. If in doubt, user should contact ITD.
- It is the users responsibility to check all external material for viruses – this includes e-mails with attachments and disks from external sources.
- It is prohibited for employees to create and distribute dangerous code – of any form within PMU and associated parties.

Internet Fraud

- Users are not permitted to use the PMU network or computer systems to perform a transaction they are not authorized to perform.
- All transactions will be logged and will be used in the event of any illegal misconduct.
- All users must always represent themselves as themselves when communicating and operating on PMU systems and network. Misrepresenting yourself is classified as a fraudulent event.
- Users are not allowed to create personal web pages using PMU facilities (systems, network or computers).

- Users must report suspected fraud to PMU\ITD immediately – this can be done anonymously.
- Users are not permitted to operate an independent web page – running an online business for personal gain is forbidden using PMU facilities.

Theft of Information

- Users must only access information which they have authorized access to.
- No information is allowed to be given to an external party unless written permission is given by PMU management.
- All information created and used in the course of the user's employment remains the sole property of PMU.
- Theft of information includes the copying of software and using it without a legal license.
- This is forbidden at PMU and can be classified as a serious act of misconduct within the organization.
- All users of software must strictly abide by copyright laws and restrictions detailed by the software manufacturer. Users must not copy software from the Internet. This includes the use of freeware and shareware (certain terms and conditions normally apply). All users must contact PMU\ITD if such software is required to perform their job.

Use of Electronic Mail (e-mail)

Electronic Mail (E-mail) Functional Policy

E-mail Content

- Unacceptable e-mail content must not be acquired, possessed, sent or shown to other employees. For definition of Unacceptable e-mail, refer to the "Expressly Prohibited Use" section in the Electronic Mail Usage Functional Policy document.
- If users are found creating, reading or distributing such mail, they will be penalized accordingly. Refer to section 9 of this document for penalties.
- All e-mail attachments must be scanned for viruses.
- Misrepresentation of oneself is prohibited within PMU– employees should always represent themselves as they are.

Representing PMU

- The use of email to create contracts for and on behalf of PMU is strictly prohibited. PMU Management or the HR Department of PMU must approve all contracts.
- E-mails must not contain any information, views or opinions of the employee's that could create a negative corporate image for PMU.
- All employees have a disclaimer attached to each e-mail. This disclaimer must expressly disclaim the employee's authority to act for or bind the employer.

Defamation

Defamation is defined as "The unprivileged publication of a statement which exposes a person to contempt, hatred, ridicule or obloquy". Defamation usually consists of written or spoken works but can also include graphics – cartoons or pictures, voice or video conferencing facilities where word is not used.

- Defamation of any person, whether they are employed by PMU or not, is strictly prohibited. This includes written, spoken or graphically representation – unacceptable e-mail content.
- Defamation will lead to a severe disciplinary action.

Copyright

Current Legislation

- In Saudi Arabia, copyright protection is afforded solely under the Copyright Act. The Copyright Act recognizes the following types of work, which are eligible for protection:
  - Literary, musical and artistic work;
  - Sound recordings, cinematographic films, sound and television broadcasts and programme-carrying signals;
  - Published editions; and
  - Computer Programs.
- Computer databases (tables and the data) are protected as literary works.
- Internet web sites are multimedia products containing written texts, photographs, pictures, etc. and all should be assumed a copyright. Web sites can also be seen as computer programs.
- Infringement of the Copyright Act falls into the following categories:
  - Infringement by reproduction;
  - Infringement by publication;

- Infringement by public performance;

Software Management Functional Policy

Software Copyright

- All users must be aware of and understand the software copyright and acquisition standards, and non-compliance to the software and standards will cause PMU to take the required disciplinary action against staff who breach them.
- PMU must maintain proof and evidence of ownership of licenses, master disks, policy's, etc.
- PMU must implement controls to ensure that any maximum number of users permitted is not exceeded.
- All users must comply with the terms and conditions for software and information obtained from the networks.
- All employees must conform to the Copyright Act as described above.
- Employees are not permitted to load an illegal copy of software on any PMU computer or related facilities.
- The viewing, discussion or distribution of pornography material either by using the facilities of PMU, being on or off the University premises, or during work hours is forbidden.
- PMU will monitor Internet web site access and logs will be maintained for 3 months.

Safeguarding of Organizational Records

- Important records of organization are protected against loss, destruction and falsification.
- Some records may need to be securely retained to meet statutory or regulatory requirements, as well as to support essential business activities. Examples of this are records, which may include evidence that PMU operates within statutory or regulatory rules, or to confirm the financial status of an organization with respect to shareholders, partners and auditors.
- The time period and data content for national law or regulation may set information retention.
- Records are categorized into record types, e.g. accounting records, database records, transaction logs, audit logs and operational procedures, each with details.
- Considerations are given to the possibility of degradation of media used for storage of records.

- Storage and handling procedures are implemented in accordance with manufacturer's recommendations.
- Data storage systems are chosen such that required data can be retrieved in a manner acceptable to a court of law, e.g. all records required can be retrieved in an acceptable time frame and in an acceptable format.
- The system of storage and handling is ensure clear identification of records and of their statutory or regulatory retention period.
- To meet these obligations, the following steps are in process:
    - Guidelines on the retention, storage, handling and disposal of records and information;
    - A retention schedule identifying essential record types and the period of time for which they retained;
    - An inventory of sources of key information and
    - Appropriate controls to protect essential records and information from loss, destruction and falsification.

Penalties

Depending on the number of offenses made and on the severity of the offense or non-compliance with the provisions covered in this document, the corresponding penalty will be applied at the discretion of the PMU Rector based on the University's By-Laws and Procedures

Internet and Intranet usage

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.

Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets (Digital Media)
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All management information systems
- All business activities supported by PMU

All of the above are either owned or leased by the PMU and under the PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy statements govern the Computer, Network and Telephone Usage Functional Policies:

- Independent review of information security in the organization must be done on a regular basis;
- The security requirements of an organization outsourcing the management and control of all or some of PMU's information systems, networks and/or desktop environments must be addressed in a contract agreed between the parties;
- Relevant information security roles and responsibilities must be documented in job definitions where appropriate;
- All Employees and third parties such as contractors, consultants, business partners and outsourced staff must sign a confidentiality agreement as part of their initial terms and conditions of employment;
- Aspects related to information security must be addressed in the Organization's standard employee's terms and conditions of employment and for third parties, with a formal contract with the PMU;
- Users of information services must be required to note and report any observed or suspected security weaknesses in or threats to systems or services;
- The violation of organizational security policies, functional policies and procedures by employees must be dealt with through a formal disciplinary process;
- Capacity demands must be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage is available;
- ITD must implement detection and preventive controls to protect information and information processing facilities against malicious software and appropriate user awareness procedures;
- Authorized PMU employees must be provided with Internet access for academic and business use;

- Content scanning must only be enforced in checking for malicious software, viruses, etc.;
- Functional policies for the use of the Internet and intranet must be implemented and controls put in place to reduce security risks created by the Internet and intranet usage;
- The implementation of the E-mail, Internet and Intranet policy is aimed at ensuring that all employees and independent contractors are made aware of the disciplinary sanctions that PMU must impose on any unauthorized and/or unacceptable use of these services;
- Employees of and independent contractors to PMU are specifically warned that personal criminal and/or civil action may be taken by PMU in the event of their breach of this policy;
- The allocation of passwords must be controlled through a formal management process;
- An intrusion detection system must be in place to detect unauthorized use of PMU networks;

All users must have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual.

Internet and Intranet Usage Functional Policies

- Access to the Internet: Access to the Internet is provided to all employees and students. Guests of the university will be provided Internet access at the discretion of the university.
- Acceptable and Unacceptable Use of the Internet/Intranet
- In an open plan office users must be aware of unauthorized users reading information displayed on their screen.

University Use

PMU sees the Internet/Intranet as significant tools for business benefit and for achieving required business objectives, i.e. The Internet can be used to access a wealth of information and resources, while the Intranet is one of the most effective ways of making PMU information available internally to the organization.

These services do however offer the opportunity for abuse of resources and inappropriate use of these mediums could expose PMU to significant risks. Therefore Internet/Intranet facilities will only be available to users after formal contracting of the Internet/Intranet functional policy. Any exceptions will be filed.

- Unauthorized attempts to break into any computer;

- Theft or copying of electronic files without permission; and
- Sending or posting company files outside the company or inside the company to unauthorized personnel.

Personal Use

PMU understands that many users work at non-traditional times, for example outside working hours and that these activities infringe on “personal time”. PMU therefore allows incidental and infrequent personal use of the Internet/Intranet within the Constraints on Personal Use noted below.

Constraints on Personal Use

Incidental and infrequent personal use of PMU's Internet/Intranet during or outside normal work hours are allowed on condition that:

- It does not consume significant amounts of the user’s workday.
- It does not consume substantial amounts of PMU bandwidth in such a way that it negatively impacts upon PMU systems, either directly or indirectly. PMU bandwidth could be impacted by distribution of for example the following:
    - Attachment types such as JPEG, JPG, AVI, etc; or
    - Chain letters, jokes, bitmaps, etc.
- It does not expose PMU to a noticeable increase in costs.
- It does not expose PMU to reputation or financial risks.

Expressly Prohibited Use

In order to prevent loss and the possibility of PMU being in violation of regulatory and statutory requirements the following Internet/Intranet related activities are prohibited within PMU:

- Carrying of any obscene, defamatory or discriminatory material.
- Material containing derogatory racial, gender, religious or hate-oriented comments;
- Libelous remarks about products or other companies,
- Defamatory remarks, including defamation of character; or
- Discriminatory language or remarks that would constitute harassment of any type.

Password Management

Internet/Intranet access to General Support systems and Public data shall require a password. All password creation and usage must be in accordance with those stated in PMU General Security Guidelines Functional Policy.

Downloading content

Users are permitted to download content from the Internet/Intranet. The downloading of content from the Internet/Intranet must however be in accordance with the following:

- Users downloading large volumes should consider scheduling these for transmission after normal working hours.
- When non-text files (databases, software object code, spreadsheets, formatted word-processing package files, etc.) are downloaded from non-PMU sources via the Internet, the following conditions must be adhered to:
    - Files must be screened with approved virus detection software prior to being used (opened);
    - Whenever an external provider of the software is not trusted, downloaded software should be tested on a stand-alone non-production machine that has been recently backed up. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine;
    - Downloaded files must be decrypted and decompressed before being screened for viruses;
    - The use of digital signatures to verify that unauthorized parties have not altered a file is recommended, but this does not assure freedom from viruses.

Representing PMU

Vicarious Liability:

Users must be aware that in using PMU Internet/Intranet facilities they are representing PMU. It is therefore important that the use of Internet/Intranet must be in accordance with the following:

- Users should consciously build and preserve PMU image when using the Internet/Intranet.
- Users may indicate their affiliation with PMU in mailing lists (list servers), chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain

words, or it may be implied, for instance via an electronic mail address. In either case, whenever users provide an affiliation, they must also clearly indicate the opinions expressed are their own, and not necessarily those of PMU.

- Users can indicate that opinions expressed are their own by the use of a disclaimer stating the following:
  "Any opinions, presented explicitly or implied, are solely those of the author's and do not necessarily represent those of the Organization's."

- Wiretapping and message interception is straightforward and frequently encountered on the Internet. Accordingly, PMU proprietary information must not be sent over the Internet unless it has first been encrypted by approved methods.
- User IDs and passwords, and other parameters that can be used to gain access to PMU information must not be sent over the Internet in readable form.
- PMU software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-PMU party for any purposes other than business purposes expressly authorized by management.
- Users should not allow others to use their user IDs and passwords when connecting to Internet sites requiring authentication (e.g. Gartner research database). If a user has no option but to allow this, the user must understand that he/she is the responsible party.

Expectation of Privacy

- Individual Practices: On the Web, one of the real dangers is a possible loss of privacy or leakage of information about user activities. Employees should be aware of the following issues relating to their privacy when surfing the web:
- When you visit a Web site, the site you are visiting can identify where your Internet connection originates. For example, if you use the Web from work, your activities can be identified as coming from PMU.
- Web sites can log all of your activity including any personal data you provide. The web site owner can associate you with this data on future visits. They may want to use this information to give you a better web experience, or they may be collecting competitive information, or both. Some web sites do not respect data privacy laws and may make the information collected from you available to other organizations. Should any of the events mentioned takes place, the Legal Department must be informed immediately.

- PMU Practices: The Internet connection provided to employees is a PMU resource. Activities may be subject to monitoring, recording, and periodic audits to ensure they are functioning properly and to protect against unauthorized use. Users must therefore note the following:
- PMU reserves the right to monitor sites (e.g. duration and content) visited by users and to detect security violations.
- PMU reserves the right to examine and access all information, created, stored or communicated using PMU information systems whenever warranted by business need or requirements.
- PMU will disclose information obtained through such examinations to appropriate third parties, including law enforcement agencies.
- Internet users expressly consent to such monitoring, recording and examination.

Internet Integrity

When using the Internet all users must comply with the following:

- All information taken off the Internet should be considered suspect until confirmed by separate information from another source.
- Before users release any internal PMU information, enter into any contracts, or order any products via public networks, the identity of the individuals and organizations contacted must be confirmed.

Electronic Fraud

- Impersonation: Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any PMU electronic communications system is forbidden.
- Disclaimer of Liability: PMU is not responsible for material viewed or downloaded by users from the Internet or other public communications networks. Users are cautioned that web pages may include offensive, sexually explicit, and/or other inappropriate material. Users accessing the Internet and other public communications networks do so at their own risk.

General Information on Wireless Networks:

- Wireless Networking now provides easy, Inexpensive, high bandwidth network services for any organizations which selects this Latest Network technology.

- Approved by IEEE Standards committee the 802.11 further enhanced to 802.11b/g/n specification detailed the frame work necessary for a standard method of wireless network communication.
- Connectivity previously had to creep up with the monopoly held" Wires" ,now the data can Fly thru the walls ,significantly increasing the Network Bandwidth & Performance.
- A recent survey by a leading Security Consulting Company has revealed that Wireless Networking has indeed increased in the current technology Savvy market by 30% and Wireless Networking is the Future Networking. But as Every Technology has its own loopholes, Security is a real cause of Concern for Wireless networks,.
- Access Points communicate with the data freely flowing in the Air vulnerable to penetrate by any unauthorized user.
- Placement of the access points is equally important, as you do your site survey for access point deployment, think about locating the access points toward the center of your building rather than near the windows. Plan your coverage to radiate out to the windows, but not beyond. If the access points are located near the windows, a stronger signal will be radiated outside your building making it easier for people to find you.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.

Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All business activities supported by PMU.

All of the above are either owned or leased by the PMU and under the PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy statements govern the Computer, Network and Telephone Usage Functional Policies listed in this document:

- Both the wired and wireless networks will be monitored for unauthorized use or devices.

Wireless Network (Wi-Fi) Functional Policy

Authentication

- All wireless stations (users/devices) must be authenticated to access a WLAN.
- If username and password authentication is used, users/devices must use strong passwords (alphanumeric and special character string at least eight characters in length).
- If a central authentication server or VPN gateway is used in the WLAN architecture, each wireless client must uniquely and successfully authenticate to the WLAN. Strong passwords must be used in this situation
- All wireless device users must be authenticated to access wireless devices and/or the desktop PC synchronization software.
- Wireless handheld devices and synchronization software must require a strong password, or both to authenticate access to the device or software. Users are required to authenticate when operating locally and remotely.
- Wireless device authentication must not be disabled.

Encryption

- All WLAN traffic must be encrypted to limit eavesdropping and ensure confidentiality.
- Wired Equivalent Privacy (WEP) must be enabled using 128-bit key or the strongest encryption available in the 802.11 b/g/n compliant product used.

Access Control

- All access to the WLAN system, including its data and resources, shall be restricted unless authorized by the PMU -ITD. Data traversing wireless networks and data accessible via wireless entry must be protected from unauthorized access, use, modification, or deletion using access control methods.
- Non-PMU employees, excluding approved vendors and contractors, must not have access to WLANs that connect to the PMU Enterprise data network.
- Service Set IDs (SSIDs) must be changed from the factory default to something that is meaningless to outsiders. SSID character strings must not reflect Member or Committee name, location, or product being used.
- Broadcast mode of SSIDs must be disabled in products that permit it so that the client SSID must match that of the access point.
- The authentication server, firewall, and/or VPN gateway must enforce access control mechanisms.

Anti-Virus Software

- Antivirus software at the perimeter will provide protection for handheld devices by scanning all entry ports (i.e, synchronizing, email, and Internet downloading) as data is imported into the device, provide online signature update capabilities, and prompt the user before it deletes any suspicious files.

Personal Firewalls

- It is highly recommended that WLAN client and handheld devices utilize personal firewall software.
- Users that access public wireless networks (e.g., in airports, conference centers, coffee shops) should install personal firewall software on all WLAN client and handheld devices. A personal firewall protects against wireless network attacks and rogue access points (e.g., Ad hoc networks, accidental or malicious association, soft access points) that can be easily installed in public areas.

Physical Security

- Access points must be physically secured upon proper configuration to prevent tampering and reprogramming (i.e., to prevent unauthorized physical access).
- Access points must be placed in secure areas, such as high on a wall, in a wiring closet, or in a locked enclosure to prevent unauthorized physical access and user manipulation. Devices must not be placed in easily accessible public locations.
- To mitigate eavesdropping, access points shall be placed strategically within the building so that the range does not exceed the physical perimeter of PMU-controlled facilities and allow unauthorized users to eavesdrop near the perimeter. Access points shall be placed to minimize or prevent the distance that the signal can travel outside the area that is under the control of the organization, including buildings, court yards, adjacent parking areas, etc.
- The transmission power of WLAN access points must be restricted to the lowest power required for coverage.
- In the event that the reset function of an access point is used, the device must be restored to the latest security settings.

Logical Security

- All access points shall be logically separated and isolated from the House Enterprise data network, such as on a different segment, in a demilitarized zone (DMZ), or in a virtual LAN (VLAN).
- WLANs must be treated as insecure counterparts to their wired associates. Access to resources on the wired network must be restricted.
- Access points shall be physically situated so that authorized users can connect, yet away from sources of interference such as microwave ovens and Blue-tooth devices.
- To keep interference to a minimum, access point channels shall be at least five channels different from all other nearby access points on different WLANs. Some coordination may be required if multiple WLANs are to be used within close proximity.
- All insecure and nonessential management protocols (Hypertext Transport Protocol (HTTP) and Simple Network Management Protocol (SNMP)) shall be disabled if not used
- SNMP settings must be set to least privilege (read only).
- Web-based management of access points shall be from pre-defined management stations controlled by access lists on the access point.

SNMP requests shall only be accepted from specified management devices.
- SNMPv3 products or equivalent cryptographically protected protocol shall be used since they include mechanisms to provide strong security.

Monitoring & Audit

- All wireless LANs and handheld devices must be routinely monitored and security audits performed to verify that security configurations comply with this policy, access points and wireless devices are authorized, and to identify unauthorized activity.
- If DHCP is used in the environment, logs shall be reviewed for static addresses to determine if rogue access points have been installed.
- Access logs and system audit trails shall be routinely monitored.
- The ITD will conduct routine controlled penetration tests or packet sniffing/wireless traffic analysis on WLANs and within the coverage area
- All access points must have Intrusion Detection Systems (IDS) at designated areas on House property to detect unauthorized access or attack.

Systems Administrators/Vendors/Users Responsibilities.

- System Administrators / Vendors are required to operate Wireless LANs and devices in a secure manner.
- System Administrator / Vendors job includes proper authorization and termination of access, proper configuration and placement of wireless components and associated security technologies, routine, random, and event-driven maintenance, support monitoring and audit functions, etc.
- System Administrators / Vendors are required to change factory default settings and use strong administrative passwords on all wireless devices to ensure a higher level of security. (On some wireless devices, the factor default password is blank.) All insecure and nonessential management protocols must be disabled.
- To the extent possible, System Administrators / Vendors shall ensure that their wireless implementation and associated security technologies are up-to-date with evolving standards and best practices.
- System Administrators / Vendors are required to maintain a list of authorized wireless device users to enable them to perform periodic inventory checks and security audits.
- Wireless users must only access information systems using approved wireless device hardware, software, solutions, and connections.
- Wireless users must act appropriately to protect information, network access, passwords, cryptographic keys, and wireless equipment.

- Wireless users are required to report any misuse, loss, or theft of wireless devices or systems immediately to the IT Department. (Planning & Control)

Minimum Security Requirements

There will further addition to the checklist in case of new release, Version or change in Technology. Each point in the section has a check box which needs to be filled with “Y” for available and “N” for not available. Please read the points carefully before filling the check boxes.

Reduce your WLAN transmitter power

This feature not on all and access points, but some allow you lower the power of your WLAN transmitter and thus reduce the range of the signal. Although it's usually impossible to fine-tune a signal so precisely that it won't leak outside your home or business, with some trial-and-error you can often limit how far outside your premises the signal reaches, minimizing the opportunity for outsiders to access your WLAN.

Authentication

Consider using an additional level of authentication, such as RADIUS, before you permit an association with your access points. Cisco access points, for example, can enforce RADIUS authentication of MAC addresses to an external RADIUS server.

Supplement on Email Accounts

Policy Statement

This functional policy covers PMU's E-mail usage. Communications and operational management of information resources and systems are essential to maintaining a high level of service to PMU Users. Therefore, security requirements will be developed and implemented to maintain control over Electronic Mail Usage.

It is each user’s responsibility and obligation to ensure that all IT resources are used only for its intended business purpose and that information contained or

transmitted via these resources are protected from unauthorized use, appropriation, or corruption.

Objective

The objective of these Information Security Policies is to secure PMU's Information Assets and staff.

Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU which includes

Purpose and Scope

To make a easy and secure policies for electronic mails being used by all PMU personals, to have a organized and professional method to follow in PMU, where it limits the usage, controls the email behaviors etc….

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy statements govern the email usage

- Email Domain of PMU: <user>@pmu.edu.sa
  (i.e. First letter of the first name then the last name / family name)
- E-mail must only be available to PMU employees and students.
- No offensive material must be sent using E-mail.
- Functional policies for the use of E-mail must be developed and controls put in place to reduce security risks created by electronic mail.
- Content scanning must only be enforced in checking for malicious software, viruses or violations.
- Formal agreements must be established for the electronic or policy exchange of information and software between organizations.
- PMU's policy on Internet, Intranet and E-mail services access and use provides that usage of these services by PMU employees must be compatible with the organisations objectives.

- The implementation of the E-mail, Internet and Intranet policy is aimed at ensuring that all employees and independent contractors are made aware of the disciplinary sanctions that PMU must impose on any unauthorized and/or unacceptable use of these services.
- The policy is also implemented to minimize the risk of civil and/or criminal liability to the organization through the unauthorized and/or unacceptable use of the E-mail, Internet and Intranet services
- Every Outgoing email from PMU should have disclaimer

Electronic Mail Functional Policies

Access to E-mail: All requests for e-mail access must be forwarded by HR to ITD Helpdesk for account creation.

Acceptable and Unacceptable Use of E-mail Business Use

E-mail communication enables PMU employees and other types of workers to send messages and memorandum between workers within PMU, and also between PMU, business partners, vendors and required domains, more effectively.
This service does however will not offer the opportunity for abuse of resources and inappropriate use of this medium, which could expose PMU to significant risks. Therefore e-mail facilities will only be available to PMU users by following the formal procedures and by accepting the policy rules.

Conditions on Academic and Business Use

Email usage in PMU for the academic and business use must be within, but not limited to the following conditions:

- Employees may not use e-mail for personal or commercial purposes.
- Access to e-mail from a PMU-owned home-based computer or through PMU-owned connections must adhere to all the same functional policies that apply to use from within PMU facilities.
- Employees shall not allow family members or other non-employees to access PMU e-mail system via linked home computers.
- Disciplinary action may occur after actions including or similar to those stated below of PMU e-mail facilities has occurred:
    - Unauthorized attempts to break into any computer;
    - Theft or copying of electronic files without permission; and
    - Sending PMU files outside the PMU to unauthorized personnel.

Personal Use

PMU understands that many users work at non-traditional times, for example outside working hours and that these activities infringe on “personal time”. PMU therefore allows incidental and infrequent personal use of e-mail

Conditions on Personal Use

Users may use e-mail for coincidental personal purposes on condition that:

- It does not consume significant amounts of the user’s workday.
- It does not consume substantial amounts of PMU bandwidth in such a way that it negatively impacts upon PMU e-mail system or other PMU users, either directly or indirectly. PMU bandwidth could be impacted by distribution of the following:
- Large e-mail messages. Users should consider using compression utilities such as Zip before sending large e-mail messages.
- Large e-mail attachments can also be placed on shared documents if it is being used for local communication, and pass a hyperlink to access the required files, which will reduce the bandwidth usage drastically.
- Attachment types such as JPEG, JPG, AVI, Chain letters, jokes, bitmaps, etc cannot be circulated using PMU infrastructure services.

Note: There are many free services on the Internet to share images and video files. Do not use university resources to distribute large files to large group of people.

Privacy of PMU E-mails.

As PMU allows the incidental and infrequent personal use of e-mail, users must be aware of the restrictions placed on the privacy of e-mail.

- Electronic mail is private and owned by the sender and each recipient account holder.
- The contents of e-mail will not be monitored, censored, or otherwise examined except:
- With specific authorization from the head of the Department as part of the required system administration;
- Investigations may require the examination and release of any document, including electronic files such as e-mail. Should any PMU user be

involved, the ITD Department will act only under the specific instructions from a business unit manager to ensure that individual rights, including rights to privacy and due process are maintained; and
- A special condition exists for users who receive e-mail associated with his/her job responsibilities and where, their direct supervisor or others in the department need to have access to their e-mail. ITD will continue to maintain the privacy of mail

Expressly Prohibited Use

The creation, transmission, receipt or storage of certain content may be in violation of regulatory and statutory requirements and are therefore prohibited within PMU. This content includes, but not limited to the following:

- Unprofessional Threats;
- Pornographic explicit material, but limited to unsolicited SPAMS being spoofed and circulated.
- Material containing derogatory racial, gender, religious or hate-oriented comments;
- Discriminatory language or remarks that would constitute harassment of any type.
- Any other comments that offensively addresses someone's age, political beliefs, national origin, or disability.

E-mail Manners

Any form of communication is most effective if it conforms to etiquette acceptable to both the sender and the recipient of the message. Therefore the following principles should be followed when using e-mail:

- Are concise - long messages often lose their emphasis.
- If you have received a message as a part of a group of recipients consider a reply to only the author rather than to the entire group.
- As with any written form of communication, attention to proper grammar, spelling, etc. will convey your message most effectively.
- Remember that even though the medium is electronic, the recipient of the message is another human.

Unsolicited E-mail

When a staff receives unwanted E-Mail (Junk Mail or SPAM), they must refrain from responding directly to the sender. Instead, they should forward such E-Mail to the IT-Help desk which will forward the case to the appropriate technical resource for remediation.

Representing PMU

Liability

Users must be aware that in using PMU e-mail facilities they are representing PMU. It is therefore important that the use of e-mail must be in accordance with the following:

- Users should consciously build and preserve PMU image when they use e-mail for communication. When applicable, users should attach the official PMU headers and disclaimers to e-mail. A disclaimer could state the following:
    - This message (including attachments) is intended for the addressee named above. It may also be confidential, privileged and/or subject to copyright. If you wish to forward this message to other, if you are not the addressee named above, you must not disseminate copy, communicate, otherwise use, or take any action in reliance on this message. You understand that any privilege or confidentiality attached to this message is not waived, lost or destroyed because you have received this message in error. If you have received this message in error, please notify the sender and delete from any computer.
- Unless explicitly attributed, the opinions expressed in this message do not necessarily represent the official position or opinions of PMU.
- Whilst all care has been taken, PMU disclaims all liability for loss or damage to person or property arising from this message being infected by computer virus or other contamination.
- The creation of business e-mail is equivalent to the creation of any other PMU document. Therefore, user must use the same degree of care and seriousness associated with the drafting of PMU documents when composing business e-mail messages.
- The quality of written or verbal communications reflects on PMU. Users should always strive to use good grammar, correct punctuation, and acceptable language.
- Users are not allowed to enter into any contractual agreement for or on behalf of PMU using e-mail.

Disclaimer of Liability

PMU is not responsible for material viewed or received by users from the Internet or other public e-mail systems. Users are cautioned that these communications may include offensive, sexually explicit, and/or other inappropriate material. Having an e-mail address may lead to receipt of unsolicited messages containing offensive content.

Electronic Fraud

As electronic fraud may be possible via e-mail, user must adhere to the following:

- Impersonation
    - Impersonation of another user when using e-mail is prohibited within PMU.
    - Users should not allow others to use their e-mail accounts. If a user has no option but to allow this, the user must understand that they will be held responsible for all actions performed on their e-mail account.

- Anonymous E-mail: Anonymous e-mail may be used in the event of:
    - A user reporting an incident due to wrongdoing caused by another PMU user may send anonymous e-mail.
    - Users requesting medical information, without disclosing their identity.

Computer Viruses

A computer virus is a software program intended to damage, delete or perform other harmful actions to a user's data. It is therefore important that users adhere to the following when receiving e-mail from an unknown source:

- Users must ensure that all e-mail attachments are scanned for viruses before opening, using approved PMU anti-virus software.
- Users must immediately report any malfunction that might be related to a computer virus to the IT-Helpdesk
- When accessing public e-mail servers (e.g. hotmail) or when connecting to public SMTP servers from a workstation that is linked to the PMU network, users must ensure that any attachments are scanned for viruses on the user's workstation.
- User must read and comply with the Protection Against Malicious Software and Viruses Functional Policy

Transmitting Confidential Information

Addressing E-mail

- When a user sends e-mail, it is the user's responsibility to ensure that the e-mail address of the recipient is correct.
- When a user recognizes that a mail item has been incorrectly addressed to him, the user should inform the sender by returning and deleting the mail.
- The user must ensure that their personal information on directories and/or address books is kept up to date.

Information Protection

- Prior to e-mailing or forwarding proprietary data, the e-mail options should be set to confidential. The message should be given the subject confidential.
- Documents containing proprietary information should be individually password protected.
- The sender and receiver should agree on the password by calling in advance. Under no circumstances should sensitive information be sent without a password.
- The sender should also ensure that the receiver is able to retrieve the message from the e-mail address to which it is sent – in terms of the software used to create the e-mail as well as any attached documents.
- The e-mail system should not be used to communicate details of the password.
- The message recipient should be asked to confirm receipt of the document.
    - In this subsection, "proprietary information" refers to information that is "confidential" and/or "critical".

E-mail Software

Only authorized email software may be used, no re-mailer (mail bomber) software will be permitted for any purpose.

Retention of E-mail Messages

E-mail shall be retained for periods that would normally apply to written or facsimiled transactions. Where precise retention periods need to be defined, they should be defined in conjunction with PMU IT Department.

Supplement on Software Copyright Compliance

Policy Statement

This functional policy covers PMU's Software Licensing and Compliance. This is to ensure that all PMU assets must be accounted for and controlled in the proper manner, for both physical and logical assets. These assets are crucial to PMU's success and must be protected by the proper controls to minimize any risk of harm, disruption of services or disclosure of proprietary information.

It is each user's responsibility and obligation to ensure that all IT resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff. Each policy statement is supported by standards and procedures to achieve a complete security framework in the PMU.

Purpose and Scope

- All Information Assets (Digital Media)
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All management information systems
- All business activities supported by PMU.
- All of the above are either owned or leased by the PMU and under the PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy Statements govern the Functional Policies on Software Licensing and Compliance listed in this document:

- Arrangements involving third party access to organizational information processing facilities must be based on a formal contract that must contain all necessary security requirements accompanied with appropriate responsibility and confidentiality undertaking. Any violations thereto must be dealt with accordingly.
- Owners must be identified for all major assets and the responsibility for the maintenance of appropriate controls must be assigned.
- All Employees and third parties such as contractors, consultants, business partners and outsourced staff must sign a confidentiality agreement as part of their initial terms and conditions of employment.
- Detection and preventive controls to protect information and information processing facilities against malicious software and appropriate user awareness procedures must be implemented.
- Formal agreements must be established for the electronic or policy exchange of information and software between organizations.
- Procedures for monitoring use of information processing facilities must be established and the result of the monitoring activities reviewed regularly.
- Control must be applied for the implementation of software on all systems.
- All data must be protected and controlled.
- Strict control must be maintained over access to program source libraries.
- The purchase, use and modification of software must be controlled and checked to protect against possible covert channels and Trojan code.
- Controls must be applied to secure outsourced software development.
- Appropriate procedures must be implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights and on the use of proprietary software products.

Software Licensing and Compliance Functional Policies

Protection of Intellectual Property

- All software and/or applications developed for PMU by third parties is the property of PMU. This must be conveyed to all third parties, which develop software or applications for PMU use, to prevent any dispute about ownership of the software once a project is completed.
- Software developed by PMU employees on company time becomes the property of PMU.

User Responsibilities regarding Software Licensing

- Purchase and use of third party software must be in accordance with third party licensing agreements. These agreements may include specific user restrictions such as:
    - The number of copies allowed to be installed;
    - The number of machines the software can be installed on;
    - The number of concurrent users of the software allowed at any one time; and/or
    - The customer support levels (onsite or phone) may also be specified within the agreement.
- Only appropriately licensed software may be placed on or used in a resource. Such software may only be for the purpose of conducting PMU business.
- Employees are to be provided appropriately licensed copies of software necessary to perform their assigned tasks. Employees must not be asked or expected to perform tasks for which appropriately licensed software has not been provided.
- Some software licenses allow for the user to make a copy for home use or home-based business use in conjunction with the business use of the software. A user of licensed software at work should not assume that such provision is in place. Prior to installing copies of software at home, employees must obtain confirmation of their rights in writing from relevant management.
- Internal Audit, in conjunction with ITD, must perform periodic reviews of software usage on PMU PC's, laptops and servers to ensure that it is in compliance with licensing agreements.
- All software found in violation must be removed immediately. Parties responsible for loading and/or using non-compliant software will be subject to corrective actions by management.
- The implementation of new or upgraded software must be carefully planned and managed, ensuring that the increased Information Security risks associated with such projects are mitigated using a combination of procedural and technical control techniques

User Responsibilities Regarding Software Copyrights

The unauthorized use, copying, or distribution of copyrighted software is not allowed.
Unauthorized acts include, but are not limited to, the following:
Making extra copies of computer based software for use on other computers unless specifically allowed through a licensing agreement;

Putting copies on a network in unprotected environments where they may be copied by others

To comply with government mandates and to ensure ongoing vendor support, the terms and conditions of all End User License Agreements are to be strictly adhered to:

- Obtaining copies of software from others without paying the appropriate licensing fees;
- Unauthorized distribution of software by electronic mail.
- All users of software on PMU Information Systems must strictly abide by copyright laws and restrictions detailed by the software manufacturer and the Agreements signed therewith.
- A copyright notice must be used to protect software or other copyrighted materials developed by or for PMU.

Obtaining and Using Software

Software Definitions

Software that can be obtained from sources other than ITD can be defined as follows:

- Evaluation Software: Evaluation software is a limited software that has some of its features disabled. This software usually allows the use of a fair number of features in order to entice a user to purchase the full product.
    - Public Domain Software: Public domain software is made available with no restrictions on its distribution or copying. However, unless there is a statement to the effect that the software is in the public domain, the user should assume the author retains the copyright to the software.
    - Freeware Software: Freeware is free and was developed to provide end users with a new application. There are no license restrictions to these programs.
- Shareware Software: Shareware is software that can be downloaded, tried and evaluated for its use, and its full-featured program can be bought at a nominal fee. If not bought, the shareware programs usually either stop functioning after a period of time or they continue working but will never have all of the features that the purchased version would have.
- Application Software: Application software is a software containing business application programs that may have been developed in-house or by a third party or may have been purchased off-the-shelf.

Evaluation and Public Domain Software

Obtaining or downloading of evaluation and public domain software from other than PMU sources is permitted only under the following conditions:

Selecting Business Software Packages

- The software must be required for a legitimate business purpose and approved by management.
- Use of the software must comply with all applicable copyright and license agreements.
- It is recommended that the software be obtained only from known vendors or suppliers, ideally those with whom PMU currently does business, or are considering doing business with.
- At a minimum, an evaluation as to the safety and reliability of the vendor or provider of the software must be performed by the person obtaining the software.
- The person obtaining the software should check it for viruses, trap doors, and other malicious code. A reasonable evaluation must be performed on a single system or in a test environment lab before deploying the software to others.
- If the software is found to be creating security vulnerabilities or causing system or network problems, the problem causing the identified vulnerability must be corrected in a timely manner or the software must be removed immediately.

Freeware and Shareware Software

Obtaining or downloading of freeware and shareware software from other than PMU sources is permitted only if the conditions laid out by this functional policy are adhered to. In addition, the following should be noted:

- Software distributed in this manner is often inadequately tested, e.g., Beta versions of software. The software may not work correctly, or may cause problems with other approved software. ITD has no obligation to support this software or resolve any problems it causes, unless arrangements have been made in advance with ITD Management;
- The supplier or vendor of such software may refuse to make modifications or provide support for the software in the future; and
- Shareware, where required, must be licensed and users must strictly abide by copyright laws and restrictions detailed by the software manufacturer. This includes the terms and conditions when downloading the shareware or freeware.

Purchasing Software

All requests for new applications systems or software enhancements must be presented to management with a Business Case with the business requirements presented in a User Requirements Specification document

- Proof of purchase is required for all licensed software installed on an PMU personal computing device.
- Proof of purchase may be demonstrated by possession of one or more of the following:
- Original purchase order (or a copy of the original purchase order);
- Receipt or packing slip from the vendor;
- Software right to use license; and
- Original serialized software CD or diskette.

Proof of purchase is not required for site-licensed software obtained through authorized procedures. However, users must ensure they are in compliance with the software license before copying or loading site-licensed software.

Proof of purchase must be kept and filed for reference and audit purposes.

Protection of Software

Protection of Computing Software

- CDs and DVDs and other removable media containing software programs must be locked in secure file cabinets when not in use.
- CDs and DVDs and other removable media containing application software programs must be kept under the custody of ITD

Return of Computing Software

- Software stored on PMU personal computing devices must be returned together with the personal computing device to PMU upon termination of employment or work contract.
- Off-site copies, including copies stored on personally owned computers (when permitted by the license agreement) must also be returned (or erased, where appropriate) at the same time.

Policy 03: Data Access

Purpose

Administrative data captured and maintained at PMU are a valuable university resource. To protect PMU sensitive data from unauthorized disclosure and inappropriate use the ERP system contains data from multiple operational areas that need to be integrated in order to support institutional business analysis, reporting, and decision making. The purpose of this ERP Data Policy is to ensure the security, confidentiality and appropriate use of all ERP data which is processed, stored, maintained, or transmitted on PMU computer systems. This includes protection from unauthorized modification, destruction, or disclosure, whether intentional or accidental. This policy applies not only to stored information but also to the use of the various computerized systems and computerized programs used to generate or access data, the computers which run those programs including workstations to which the data has been downloaded, and the monitors and printed documents that display data.

Definitions

ERP Data – Any data that resides on, is transmitted to, or extracted from any ERP system, including databases or database tables/views, file systems and directories, and forms.

ERP Security Administrator – An IT professional position in the IT Department is responsible for processing approved requests.

ERP System – Human Resources, Finance, Student, Financial Aid, Luminas, Executives reporting tool, Banner Online Reports, ERT and any other interfaces to these systems.

Data Owners - Data Owners are responsible for determining who should have access to data within their jurisdiction, and what those access privileges should be. Responsibilities for implementing security measures may be delegated, though accountability remains with the owner of the data.

Area of Responsibility Data Owner(s)

Student System	:	Student Affairs Dept.
Student Financial Aid System	:	Budget and Accounting Dept.
Finance System	:	Budget and Accounting Dept.
Human Resources System	:	HR Dept.
Faculty Academic	:	Student Affairs Dept.
Accounts Receivable	:	Budget and Accounting Dept.

Data Custodians - Data Custodians oversee data management functions related to the capture, maintenance and dissemination of data for a particular operational area. They are responsible for the general administration of user access to data within their area(s) of responsibility. Data Custodians are appointed by the respective Data Owner.

Data Users - Data users are individuals who access ERP data in order to perform their assigned duties or fulfill their role in the PMU.

Query access – Access enabling the user to view but not update ERP data.

Maintenance access – Access enabling the user to both view and update ERP data. This access is limited to users directly responsible for the collection and maintenance of data.

Data Administration

By University policy, certain data is confidential and may not be released without proper authorization. All PMU ERP data, whether maintained in the central database or captured by other data systems, including personal computers,

remains the property of PMU. Department heads are responsible for ensuring a secure office environment regarding all ERP data. Department heads will review the ERP data access needs of their staff as it pertains to their job functions before requesting access via the Banner Access Request Form. ERP data (regardless of how collected or maintained) will only be shared among those employees who have demonstrated a job related need to know.

Access to ERP Data

Below are the requirements and limitations for all PMU Divisions/Departments to follow in obtaining permission for access to ERP data. Division/Department heads must request access authorization for each user under their supervision by completing and submitting a Banner

Access Request Form

Approved requests will be forwarded to the ERP Security Administrator for processing. Under no circumstances will access be granted without approval of the appropriate department heads.

Secured Access to Data

ERP security classifications will be established based on job function. Specific capabilities will be assigned to each security classification. Each user will be assigned a security classification. Some users may be assigned several security classifications depending on specific needs identified by their Division/Department head. The use of generic accounts is prohibited for any use that could contain protected data.

Policy 04: Data Protection

Purpose

To protect PMU sensitive data from unauthorized disclosure and inappropriate use.

Policy Statement

It is the responsibility of each individual with access to sensitive data resources to use these resources in an appropriate manner. Additionally, it is the responsibility of each individual with access to sensitive data resources to safeguard these resources. Methods of safeguarding sensitive data include:

- Sensitive data should not be stored on personal desktop or laptop computers since these computers tend to reside in less secure locations than central servers.
- Access to computers that are logged into central servers storing sensitive data should be restricted (i.e. authenticated logins and screen savers, locked offices, etc.).
- Access to sensitive data resources stored on central servers should be restricted to those individuals with an official need to access the data.
- All servers containing sensitive data must be housed in a secure location and operated only by authorized personnel.
- Copies of sensitive data resources should be limited to as few central servers as possible.

- Sensitive data should be transmitted across the network in a secure manner (i.e., to secure web servers using data encryption with passwords transmitted via secure socket layer, etc.).
- Any accidental disclosure or suspected misuse of sensitive data should be reported immediately to the appropriate University official.
- All the critical data will be available in the application for one year and will be archived according to the backup policy.

Definition

Sensitive Data - any information that could cause an individual personal financial harm if disclosed and used improperly. Examples of sensitive data include but are not limited to social security numbers, credit card numbers, computer passwords, and any personal information flagged for non-disclosure.

Policy 05: System Development Life Cycle (SDLC)

Policy Statement

This functional policy covers PMU's Systems Development and Maintenance. It is essential that security is built into information systems and not bolted on afterward. Therefore ITD will document the security and control requirements to be determined during system design, development of the system architecture and to be implemented in the final system. Effective security related change control procedures will be in place to ensure changes occur to the system in a controlled and secure environment with minimal risk to the "live" environment.

It is each user's responsibility and obligation to ensure that all IT resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.

Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets (Digital Media)
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All management information systems
- All business activities supported by PMU.
- All of the above are either owned or leased by the PMU and under PMU's possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Systems Development and Maintenance Functional Policies

Roles and Responsibilities

Project Management

The Project Managers responsibilities include, but are not limited to the following:

- Provides overall direction for the project;
- Ensures appropriate representation of affected users and business units if necessary;
- Monitors and controls costs and project timetable; and
- Ensures deliverables are a quality product.
- Ensure adequate implementation of security policies.

Project Planning

Purpose of Project Planning

Planning must be done for development of new systems/applications and for any major and/or minor enhancements to systems/applications.

Creation of Project Plan

Project Plan creation must include consideration for the following:

- The allocation of personnel and information resources needed for analysis, design, implementation, administration, and maintenance.
- The plan must include a discussion of specific goals as an integral part of the system requirements. This must include:
- Documentation of known constraints, which could impede proper development;
- Processes to ensure adequate security has been addressed, such as security reviews.
- All cost estimates must include the cost of analysis, design, implementation, and ongoing administration and maintenance.
- All time estimates must include a reasonable estimate of the time required for a thorough analysis and implementation.
- The planned reporting structure and hierarchy must include the appropriate management levels needed for approval and control throughout the project, including:
- Requirements will be defined, and specifications approved by the Owner prior to acquiring or starting development of any applications; and
- Recoverability processes must be considered during planning since this could influence the selection of computing platforms and database management systems.

Analysis of the System/Application

Purpose of Analysis

Analysis defines the features and functions of the system or application and provides the logical system specifications from which requirements will be defined.

Analysis

The following must be included during the analysis:

- A risk analysis to determine the controls required for the system or application under development or acquired, including:
- Performing a threats and vulnerability analysis. Security vulnerability considerations including those introduced when designing the connectivity or interface with other systems and applications; and
- Performing a business impact analysis. This must include an analysis of the impact on both existing and new systems and of opening new connections
- In defining the required operating environment, existing operating system security controls must be utilized (where available).
- The environment selected must support all requirements of the system or application being developed.
- Where an application or system has no specific requirements, a statement to that effect should be documented and approved by management.
- The analysis must balance user's requirements with required security controls.
- An acquisition vs. development analysis must include specifications for required academic and business need.
- Any Request for Proposal or Request for Information used to solicit vendors must include selection criteria for functionality.

Design of the System/Application

Purpose of Design

- Design uses the logical models from analysis and makes them executable.
- The work done in design provides the basis for actual development of the system or application. System and physical architecture, interfaces, policy processes, and documentation are design components.

Requirements in Design

For all systems designed within or for PMU, requirements must be used, which have been determined in the analysis phase, prior to the application development phase. During the system design phase, Information Owners, PMU and Information Security must determine the proper control environment of the application by using the security specifications of the analysis phase.

Development Environment

Securing Source Code under Development

For securing source code under development the following must be adhered to:

- Source code, including parameter and configuration files, is a valuable information asset and must be protected when in development.
- Access control to the development environment and authorization control for all data and source code files must be implemented.
- Developer access must be restricted to only those resources required to perform established job duties.
- Security audit records capable of providing sufficient information for after-the-fact investigation of loss, impropriety or other inappropriate activity must be generated and reviewed.
- Source code under development may be at greater risk of being acquired before all copyright protection is in place, thus making it subject to claims of ownership by intruders.
- Programmers must maintain documentation of their program development and changes in order to legally support claims of ownership for software not yet copyrighted.
- Systems/applications documentation must be prepared and maintained throughout the development/maintenance lifecycles to ensure continuity.

Management of Changes to Source Code under Development

Management of changes to source code under development must conform to the following:

- Version control must be utilized for ensuring ongoing management of changes to the source code. An automated process with specific version tracking functionality or a policy procedure may provide version control.
- Source code under development must be backed up and secured from unauthorized access.
- Changes to source code must allow for rollback. Rollback will enable the developer to restore source code to its original state if necessary.
- Changes to source code under development must be part of the change control process.
- System/Application documentation should be updated when changes are made.
- Changes to source code must be evaluated by a second person to review if any inappropriate code has been included (i.e. Trojan horses, etc).

Test vs. Production Environments

The following must be adhered to for the test and. production environments:

- Development and testing must be performed in an environment which is separate from production, either physically or logically, to ensure that testing and production processing cannot impact each other.
- If possible, testing should not involve any components of the production environment, including software, hardware, and network connectivity.
- Testing should be done only with test data; production files and data must never be impacted by the development process.
- If access to production environment is required, such access must be approved by the Information Owner and must be limited to read only.
- Copies of production data may be used for testing, after scrambling where feasible, if they are controlled to the same degree as in production.
- Sensitive data should be sanitized or deleted from the created test data.
- Production processing must be performed only with production data. Production data must never be impacted by the testing process.
- Development hardware must not be migrated to a production environment until all development and testing is completed and proper signoff was obtained.
- It is recommended that the operating system and all file systems be reinstalled and reinitialized to ensure that all production security controls are in place.
- Measurements need to be in place to ensure that the tested system is transferred to production without any alterations (e.g. using checksums).

Testing of the System or Application

Purpose of Testing

- Testing verifies that the features and functions of the system or application are in line with the development specifications and ensures that its operation is compatible with the environment in which it will run.
- During testing, the test scenarios are designed for unit, system, integration, and acceptance testing.
- All tests are executed and the results are logged and evaluated. All errors must be corrected during testing and before implementation.

Security Requirements for Testing

Security must be integrally included in unit, system, integration, and user acceptance tests. This includes both developed and purchased software. In all cases:

- Test plans must include time and resources to sufficiently test all aspects of the security functionality.
- Scenarios for testing security must be designed in attempt to defeat or circumvent security.
- Testing procedures must be properly documented on the change request forms.
- During integration and acceptance testing, logical access restrictions must ensure that developers have no update access and that the code being tested cannot be modified without written consent of the user.
- Both successful and unsuccessful access attempts must be tested and the appropriate audit logging must be verified.
- The developer must supervise unit testing in the testing environment. The developers manager must then perform an independent review of these results.
- As part of the test, verification must be done to ensure that the newly developed system or application does not introduce vulnerabilities in existing structures, common networks and systems.
- If test data must be transmitted to an external site, other than to the ultimate recipient, to complete a test, all sensitive or proprietary information in the data must be sanitized or deleted.
- If the system or application is intended to execute on more than one type of platform, security must be tested in each of the possible operating environments.
- Testing of security administration functions is required.
- If the software being tested was purchased, it may be advisable to have a technical representative from the vendor onsite during the testing.
- The system or application must be tested when the security function is down to ensure that access is not allowed.
- All testing logs and evaluations must be secured and marked.
- Where a mechanized scanning tool is available, a vulnerability scan must be completed for all new systems prior to being approved for production. The tools used for such scans must not be distributed to the developers or any persons other than security or system administrators.
- All significant modifications, major enhancements and new systems must be integration and acceptance tested prior to installation of the software in production.
- Volume and stress testing for the security functions must be included in the test plan. If possible, maximum user access should be simulated to measure the response of the system.
- Backup and recovery processes for the system or application and for any databases must be tested.
- Disaster Recovery Plans must be tested and updated to ensure changes to systems/applications are adequately addressed.

- All tests performed must be signed off in the test plan/test script by staff who performed the test and must be approved by the Business Owner.

Unit Testing

- The developer will supervise unit testing in the development environment.
- Testing procedures must be properly documented and the developer's manager must perform an independent review of unit test results.
- If problems are noted, the developer will document the problem, make appropriate modifications in the development environment.

Integration Testing

- All significant modifications, major enhancements and new systems will follow integration testing prior to installation of the software in production.
- System stress testing and volume testing must be performed, and in some cases, parallel testing will be required.
- Integration testing must be conducted in a separate, independently controlled environment.
- During integration testing, logical access restrictions must ensure that developers have no update access and that the code being tested cannot be modified without the written consent of the user.
- Copies of production data, sanitized from any customer data, or pre-designed test datasets must be used for testing purposes..

User Acceptance Testing

- All significant modifications, major enhancements and new systems must be acceptance tested by the appropriate users, prior to installation of the software in production.
- The user acceptance plan will include tests of all major functions, processes and interfacing systems.
- Testing procedures must be properly documented on the change request forms.
- During acceptance testing, logical access restrictions must ensure that developers have no update access and that the code being tested cannot be modified without the written consent of the user.
- If problems are noted, the user will document the problem, the developer will make appropriate modifications in the development environment and submit it to CASD for re-testing.

Implementation of the System or Application

Purpose of Implementation

- Implementation installs the system or application into production.
- During implementation, data is converted as needed, and live processing begins.
- Users and operators should be trained before implementation.

Requirements for Implementation

Before moving a system or application into production, the following must be accomplished:

- An operational readiness review must be completed which includes evidence of the following items at a minimum:
    - Compliance with the current PMU IT Architecture;
    - Satisfactory completion of vulnerability scanning, where feasible;
    - Preparation of a Disaster Recovery/Contingency Processing Plan; and
    - Assignment of an appropriate number of qualified System and Security Administrators.
- A backup of all existing files and databases that will be impacted must be done before beginning implementation.
- After successful installation, all developer access must be removed to the production environment.
- If multiple sessions were allowed for any testers or other users, they should be reviewed in production and limited if no longer needed or conflicts with existing access.
- Approval to move software from development to production must be obtained.
- Approval to move software from production to development must be obtained within the formal change management process.
- Security administrators and users must be fully trained on the new functions.
- Any policy security processes required for implementation must be in place.
- Availability of a facility to print security reports, such as:
    - Security violations;
    - User profiles and access rights; and
    - User administration activities.
- Personnel to review and monitor audit intrusion reports must be available and trained.

- For purchased software, a written vendor statement that all security controls have been successfully implemented and are functional must be obtained.
- Only object code should be distributed to end users.
- Rollback plans need to be in place.
- License data on all purchased software distributed must be maintained.
- If the new system or application is replacing an existing system, procedures for maintaining security administration on both systems during the implementation must be established.
- Ensure the correct version is installed (the version that was tested and signed off).
- Ensure the necessary SLA is in place and signed.

Maintenance of Systems or Application

General Maintenance Information

General maintenance information includes:

- Maintenance of systems and applications begins after the system or application is stable and no longer under development and continues over the life of the system.
- It includes day-to-day system/application monitoring, tuning for performance purposes, scheduled and emergency maintenance functions, problem management to correct faults and to adapt to business change, change control for system enhancements, and security administration.
- Maintenance actions must be planned and must sufficiently cover the maintenance of security functionality of systems/applications.

Monitoring of Systems and Applications

Monitoring of systems and applications must be in accordance with the following:

- Systems and applications are only valuable if they are available at the required times. All parties involved must ensure that procedures to support operational monitoring of all production systems and applications are in place.
- Dated and time stamped logs should be produced to aid in evaluating the operations. Examples of areas to monitor include:
    - Outages and downtime;
    - Volume of usage for data and users;
    - General system response time; and
    - System and resource access.

Emergency Maintenance Procedures

Emergency procedures for correcting unpredicted software errors must include:

- The ability to grant sufficient access to enable the maintenance personnel to accomplish the task.
- As soon as the emergency is past, details of the changes implemented must be documented.
- This documentation should include the following details:
    - The change requestor;
    - Authorization for change;
    - Short description of the required change; and
    - The time frame in which the change was required.
- Normal maintenance or change control procedures should be applied retroactively.
- Emergency changes to programs should be made to separate copies of the programs to allow production work to continue.
- After the emergency, implementation approval as used in change management should be utilized.
- If it was necessary to grant special access to production resources, activities must be monitored and logged. After the emergency, all such access must be revoked.

The installation of any type of back door that circumvents security controls is prohibited.

Policy 06: Change Management

Policy Statement

Prince Mohammad University relies upon IT services in order to perform its roles of teaching and administration. The inter-dependencies of these systems are complex and the results of change made to any system may have serious consequences. The uncontrolled implementation of changes to University's IT systems, critical systems and underlying infrastructure utilized to perform its core roles presents a significant risk to the University.

Changing system requirements, resolution of known issues, implementation of new services and routine maintenance all require appropriate Change Management. Change management ensures the stability of systems by the identification and mitigation of associated implementation risks, minimization of disruption to Prince Mohammad University's operations caused by system outages,
and improves service and service levels provided to the University.

The Change Management policy is based on the industry best-practice standards of ITIL – the IT Infrastructure Library.

This policy outlines the ITD Change Management process, including its roles and accountabilities.

Purpose

The goal of Change Management at Prince Mohammad University is to ensure that standardized ITIL (IT Infrastructure Library) methods and procedures are used for efficient and prompt handling of all Changes to the IT systems; thus minimizing any undue disruption to IT services delivered to the University.

Change Management also aims to provide the ITD the ability to rapidly adapt as University's requirements change and increase their ability to ensure a customer focused operation is maintained

To ensure that a comprehensive business and technical risk assessment is made for all changes, allows for open communication between key stakeholder and coordination of resources required for successful implementation.

Definitions

PMU: Prince Mohammad University

ITD: Information Technology Department

ITIS: IT Infrastructure Services

Change Management: is the process of developing a planned and documented approach to change in an organization. In the ITIL framework, Change Management is responsible for controlling change to all configuration items within the live environment, test and training environments, and all environments under the control of ITD operations. It is not typically responsible for change within development projects where change requests are managed by the Project Manager.

CAB: The **Change Advisory Board**. As can be inferred from the name, this body has no governance role, but is tasked with *advising* the Change Manager and Service Owner of the perceived impact of a requested change. This body is made up of a core group with representation from all major systems and the core Services teams, and incorporates required stakeholders depending on the nature of the Request for Change being assessed.

ITIL: The **IT Infrastructure Library** is a collection of internationally recognized best-practices for delivering IT Services, covering all aspects of service provision, quality assurance, and providing a framework which allows customization of internal processes. It was developed within the British Public sector and has since been revised with commercial input to become the world standard for IT Service Management.

RFC: Request for Change – an electronic form which initiates the Change Management process.

CM (Change manager): is a Chair of the Change advisory board

Meeting and will be responsible to select the Change advisory board members per the nature of the RFC. CM is also responsible for scheduling and publishing approved changes.

Service Owner: is a person or department responsible to provide the service for the business.

Change Management Process Development

Guidance from ITIL

The Change Process at the Prince Mohammad University has been based extensively upon the guidance of the British Government "Information Technology Infrastructure Library" textbooks (ITIL). Wherever possible, this guidance has been followed closely, most notably in the use of the ITIL terminology.

The ITIL texts provide comprehensive guidance as to industry best-practice in this area, and have been widely adopted as standards to ensure IT infrastructure stability and resilience.

ITIL forms the basis of the British Standard BS15000 and International Organization for Standardization ISO20000.

Process Development

The Change Management Process was developed within the ITD and implementation will be staged. The benefit of this approach is to work on the process iteratively, allowing various approached to be trialed before formal adoption

Process Improvement

The Change Management Process will undergo continuous improvement. The primary source of improvements will be the review phase of the process, wherein

the Change Advisory Board members analyze and identify process improvements which will enhance success or increase the efficiency of the process.

Constructive feedback is welcomed, and suggestions for improvement will be incorporated wherever value is added.

Change Management Process Notes

Change Process Scope

Currently the scope of this process is limited to ensure a successful staged implementation. All changes to centrally manage IT infrastructure and Systems must follow the PMU Change Management Process.

This scope is further limited to changes for which an outage or noticeable change is visible for clients. This ensures the process is not swamped by minor operational changes, and reduces the bureaucratic overhead of the process.

Integration with the (Purchase Department) Approval Process

Where Purchase Department approval is required for IT equipment or software purchases, an assessment of the impact of the purchase should be sought through the PMU Change Management process. The appropriate place for this integration is prior to distribution of Request for Proposal made by Director of IT

In some instances, assessment may be requested to provide information for inclusion as part of the development of the business case.

Change Type

The type of the changes which follow the Change Process varies. The following categories have defined:

- Pre-approved
- Minor
- Medium
- Major
- Urgent
- Emergency
- Installation
- Evaluation

The type of the Request for Change (RFC) affects the timeline of the request, determines the notifications which must be sent, and the review and closure process to follow.

Pre-Approved Changes

Many changes do not require authorization, and do not need to pass through the formal process. Those changes should still be logged in the normal manner; however they will proceed to the scheduling phase immediately.

This is essential to ensure appropriate change scheduling, and the minimization of impact arising from change conflicts. It also provides and audit trail of improvement made to systems and services. In Change advisory board review phases the minor or medium changes done frequently can be categorized as Pre-Approved Change.

Minor or Medium Changes

Minor or medium changes follow the standard change process and may affect relatively few clients or cause minimal impact; however they do require proper notification of selected groups of staff or students.

Major Changes

Major changes are designated as such because the affect, or have the potential to affect, large numbers of clients, or will involve lengthy outages of critical systems.

Major changes will typically involve notification of all staff or students and may require authorization by Senior University Management (IT supervisory committee, Communication meeting)

Urgent Changes

Urgent changes are designated as those which are not able to follow the standard change implementation timeline. These may occur due to external factor such as consultant availability or external project critical timelines, possible

hardware failure, or simply due to scheduling issue necessitating implementation in conjunction with other previously scheduled changes.

As these changes fall outside the normal change window, a special meeting of the Change advisory board may be held, or consultation prior to approval may be made by email.

All urgent changes will be reviewed by the Change advisory board post-implementation. This will ensure that appropriate measures are taken to reduce or eliminate the requirement for such urgency.

Emergency Changes

Changes may be designated at the time of recording as 'Emergency' changes. These changes will not be required to follow the standard Change Management Process, but instead are automatically approved and proceed directly to implementation. Emergency changes naturally take schedule precedence from all other changes.

All emergency changes are reviewed by the Change advisory board, following implementation.

Installations

All new systems to be commissioned within the IT managed server facilities must be submitted as an RFC. This allows the Change advisory board to assess the request for business and technical risk and ensure appropriate resources are allocated. It also automates the creation of appropriate work requests to ensure all standard tasks for preparation take place.

Evaluations

The process for the evaluation of a new item of equipment or software prior to its sale or support is important in order to ensure support criteria are met. The inclusion of a change type for the evaluation of new equipment etc reflects this importance, although it constitutes a variation on the standard process.

Request for evaluation are circulated to a number of key areas of ITD, to ensure appropriate checks take place prior to introduction.

The Change Advisory Board

Overview

The Change Advisory Board (CAB) is the body responsible for the assessment of changes to determine their risks and impact, and authorization of RFC implementation or otherwise.

Given the complexity of computing environment a Change advisory board has to be developed which has the depth to ensure accurate assessment and identification of risk and impact, both from a business view point, and technical and support issues. The method chosen in this instance has been to establish a "core" Change advisory board of relevant staff from the IT infrastructure services and mission critical MIS system, which will almost always be involved in change assessment, and then bring other appropriate stakeholders into the assessment when required.

The members of the core Change advisory board:

- Change Manager
- Manager - Infrastructure Core Technologies
- Manager – Management of Information Systems
- Manager – Academic Computing Services
- Business Representative

In essence the Change Advisory Board has a dynamic membership so we do not waste the time of those that particular changes do not impact upon. This follows the industry best-practice guidance provided by ITIL.

Additional Change Advisory Board members relevant to each change are added to the group based on the services affected by a particular RFC. In particular this includes the service owners of all affected services. A further list of stakeholder for inclusion in the assessment includes representation from all service units and academic colleges and is built in consultation with those units. It may include a technical support of management staff with vested interest in the service

This stakeholder will be given the opportunity to submit an assessment of relevant changes, however they will not be required to attend the regular Change Advisory Board meetings, although they are welcome to do so.

Change Advisory Board Responsibilities

- The responsibilities of the Change Advisory Board members are:
- Identification of business , technical and support risks associated with the implementation of the RFC
- Identification of the direct or indirect costs and resource requirements

- Identification of impact on any other University services
- Identification of impact on PMU operations not directly associated with the change
- Circulation of assessment and collation of responses from team members
- Timely response to requests for assessments
- Assisting the Change Manager with authorization of RFCs

Change Advisory Board Meetings

The Change Advisory Board will meet weekly to perform authorization, review and closure of RFCs. The Change Manager is responsible for scheduling and rescheduling the meeting.

Time frame

As the Change Advisory Board meets weekly, impact on timeframe for implementation should be minimal, given appropriate planning prior to RFC initiation.

Agenda

The Change Advisory Board meeting will be chaired by the Change Manager, and will follow a standard agenda.

Authorization

Discuss RFCs in assessment phase
Approve or Reject RFCs

Scheduling

Schedule changes
Ensure ITS Change Calendar is updated

Notifications

Ensure all RFCs include proper notification
Emergency and Urgent RFC Review

Closure

Close all outstanding completed RFCs

Review

Review failed changes
Improve the IT Change Management Process

The agenda of RFCs for assessment will be circulated to Change Advisory Board members and notified via email prior to each meeting.

Urgent Meetings

An ad-hoc urgent Change Advisory Board meeting may be called as and when required for urgent changes. This may be conducted via email if required.

Quorum

For IT infrastructure changes, a quorum of four Change Advisory Board members must be present in order to authorize any RFC. In the absence of sufficient Change Advisory Board members, all changes may be deferred until a time a quorum can be obtained or referred to Service Owner and Director of IT to authorize.

Authorization

For an RFC to be authorized, it must be approved unanimously by the Change Advisory Board, having taken into account the assessments submitted. Should a unanimous decision be unachievable, the RFC will be referred to Service Owner, IT Director for a final decision.

Reporting

An essential element of the Change Management Process is the requirement to ensure the IT supervisory Committee and Senior Management are well informed about all Changes relating to mission critical systems, especially those for which they have delegated accountability.

The Department heads and Service Owner identified for each MIS system are to be included in automated reporting. The Forward Schedule of Changes will also be circulated to ITD Management and Senior Administrators monthly.

Process Overview

Initiation / Recording

Due to the variety of the changes that may be required, specific Request for Change forms is designed to suit the type of change. They are as follows (see Appendix A for templates):

The proper recording of changes is essential to this process. All changes must be submitted either electronically or by tools approved by PMU.

RFCs must be filled out in full and include the following information:

Initiator	The person requesting the change should fill in their user id. All communication with the initiator will then be made by email
Service Affected	To identify the Owner and stakeholders of the service which are to be consulted and given the opportunity to take part in the RFC assessment.
Requested Date	This indicates the data and time on which the initiator wishes to implement the change. Both date and time are required to assess the impact of outages.
Critical Date	In most cases the requested date will become the implementation date. The exception to this is when the request conflict with higher priority change already in the system, or when another critical date is indicated by the assessment. The critical date should be the date by which this change must be implemented. It will be used to resolve scheduling conflicts only
Change Description	Describe the requested change in detail, providing as much information as required for other staff to understand and make an appropriate assessment. This change description should include details of the implementation plan, if appropriate.
Reason for Change	Why is this change being requested? Is It to fix a known problem?

	If so provide the provide the problem number.

Who will this Change effect?	The RFC initiator should provide their assessment of the impact of this change. Which clients will be affected? Will other services be affected? Which staff will be required for the implementation? The Change Advisory Board will ensure appropriate representatives from this list provided are advised of the change and allowed an opportunity to provide their assessment.
Length of an outage	If there is to be an outage associated with this Change, please indicate the length. Approximation should be accompanied with some explanation.
Back out plan	If the change implementation fails, what plans have been made to reverse the change? These plans should be comprehensive, as in the case of a failed change, they will be reviewed by the Change Advisory Board to identify area for improvement.
Change Type	Indication of the type of RFC: Pre-Approved , Minor , Medium , Major , Urgent or Emergency
Notification Text	What message should be sent to the clients?

Filtering

It is essential that indicated fields are filled in, and the system/CM will not save the requests without identification of the initiator, change description, requested date and back-out plan.

The above filtering can be done at form level or by using tools approved by PMU. policy Filtering of RFC also takes place to ensure changes are not submitted to the process which are erroneous and frivolous or requested by unauthorized staff.

Initial errors in the completion of the RFC form must be quickly identified, as must any missing information. RFC record may be updated by the Change Manager, Change Advisory Board members, or the RFC initiator. All changes made will be logged to ensure proper audit trail.

Inputs

Completed RFC form

Output

Filtered and corrected RFC

Roles and responsibilities

Responsibility for filtering the RFC form and ensuring accurate information has been recorded lies with the Change Manager. In the absence of the Change Manager this responsibility lies with the members of the core Change Advisory Board.

Assessment

Assessment is one of the key phases of the process. Request for change will be forwarded via email to the Change Advisory Board members for their assessment. The Change Advisory Board is responsible for assessing the RFC and providing their assessment of:

- Business and technical risks associated wit the RFC
- Impact on any other PMU Services
- Impact on PMU operations not directly associated with the change
- Direct or indirect Costs and resource requirement

Email notification will be sent to all core Change Advisory Board members , the Service Owner , and identified service stakeholders following successful RFC and collation of responses from other affected colleagues (where necessary).
The notification of assessment can be forwarded to other staff members if required.
Change Advisory Board members have a responsibility to ensure they respond to requests for assessment in a timely manner. Should no response be submitted, it will be assumed that no impact is foreseen in their area and therefore they approve the RFC.

Requests for further Information

Change Advisory Board members may also use email to request more information from the initiator. The initiator may respond by email. Following response, the Change Advisory Board will be informed of both the question and the answer provided to assist with their assessment.
This will highlight areas of the RFC where clarification is required and may also result in revisions to components of the process itself.

Inputs

RFC

Outputs

Change Advisory Board assessment
Assessed change for authorization

Roles and Responsibilities

The change Advisory Board members have a responsibility to assess all RFCs to the best of their ability and knowledge.

Assessment should be provided within two working days of notification

Categorization

Taking place in parallel with the assessment phase the RFC is categorized on a number of aspects.

Source

The source of the change is categorized in order to identify whether the RFC is the result of a fix to a known problem, a new service, an installation, a patch or upgrade, or a client requested enhancement.

Service

It is important that the service to be changed is identified, as this allows the identification of relevant stakeholders who would then be requested to take part in the assessment.

Impact

The impact of the change is the extent to which it affects PMU's operations, based roughly on the number of clients affected by the change, or the business critical nature of the services affected.

Urgency

Urgency provides an indication of the extent to which delay of implementation can be tolerated

Priority

The combination of Impact and Urgency allows us to priorities RFCs appropriately; ensuring resources are targeted where they are most needed and eliminating scheduling conflicts.

Scale

The scale of the change gives the Change Advisory Board an indication as to the level of authorization required.
These categorizations are important to monitor the nature of changes, and to ensure efficiency of the process. They also contribute to the approval and scheduling phases of the process.

Authorization

Following assessment by the Change Advisory Board, the RFC will proceed to authorization. All RFCs are authorized by the Change Advisory Board during the weekly meeting or by special arrangement if the RFC is designated urgent. Authorization will be based upon the collected assessment made by the Change Advisory Board members , and will balance the expected benefits of

implementation with the business and technical risks identified, the urgency of the change and the predicted impact on clients or PMU operations.

All changes to centrally manage IT infrastructure will be authorized by the Change Advisory Board itself. In the case of RFCs which are for MIS systems, a recommendation for approval or rejection, and the Change Advisory Board assessments will be forwarded to the Service Owner or appropriate authority for formal sign-off. Those changes which will impact on several critical MIS systems will be referred to higher authorities depending on the scale of the change.

For an RFC to be authorized, it must be approved unanimously be the Change Advisory Board, having taken into account the assessments submitted. Should a unanimous decision be unachievable, the RFC will be referred to the Service Owner and Director of IT for a final decision.

Following the Change Advisory Board meeting the appropriate RFC will be updated, setting its status to Approved or Rejected, and specifying any points noted by the Change Advisory Board during the discussion.

Approval of the RFC will result in the notification of the Change Advisory Board members, the Service Owner, the Initiator, Director of IT

Rejection of the RFC will result in notification of the initiator with the reason for rejection.
No unauthorized RFCs will be implemented. The decision of the Change Advisory Board or Service Owner will be final. The RFC may be re-submitted provided that all the issues resulting in the rejection have been mitigated.

Inputs

• Change Advisory Board assessments
• RFC

Outputs

• Recommendations for approval or rejection to the Service Owner.
• Approval or rejection notification to the Initiator,
• Notification to ITD Management
• Notification to Service Owner
• Notification to Change Advisory Board members

Scheduling

Proper scheduling is important to ensure change implementations do not conflict and cause undue impact on the PMU operations.

The IT change calendar should be published on the Intranet. This should be the definitive source of change schedule information, and is updated automatically directly from the Change process.

Changes requested for implementation within the same time period are rescheduled based on the impact and urgency of each change

Input

Approved Changes
Existing Change Schedule

Output

Updated Change Schedule

Roles and responsibilities

Scheduling is the joint responsibility of the Initiator, the Service Owner and the Change Manager.

Notification

All notification to Clients should be broadcasted. This ensures consistency and reliability in notification process and content. This is especially important where outages may affect client operations, or where an outage to normal service is involved.

All notification will include reference to the appropriate RFC and links to the ITS change Calendar.

Notifications will only be sent following proper change authorization.

No change notification to be sent by any other party.

All RFCs which are rescheduled must be notified to clients, firstly to inform them of the cancellation of the original change or outage window, and then to provide details for the updated schedule.

Inputs

Scheduled Change
Notification text via RFC

Outputs

Notification to appropriate client groups

Roles and responsibility

Responsibility for notification lies with the IT help Desk / or the Change Manager.

Implementation

- From a change management point of view, the implementation of the change should follow the plans provided as part of the RFC.
- Success or failure of the implementation must be promptly reported to the IT
- Helpdesk, as must any known issues created by the implementation.
- Following the scheduled date of implementation, an email message will be sent to the initiator requesting a status update.
- On the requested implementation date, a problem record will be created and all incidents attributed to this implementation will be recorded efficiently which will provides raw data for change review phase.

Inputs

Authorized and Scheduled RFC

Outputs

Successful or failed change
Problem record with associated incident

Roles and responsibilities

The Initiator has responsibility for ensuring the implementation follows the suggested plan, and that back out plans are implemented if required. They are also responsible for ensuring appropriate staffs are available to assist with implementation, when and if required.

Review

All changes which fall into the following categories are reviewed:

- Failed Changes
- Changes which exceeded the specified outage window
- Emergency or urgent changes
- Changes causing unexpected or unreasonable incident volumes

Changes falling into these categories will be passed to the Change Manager, who will ensure appropriate investigation take place, circulate a written report, and facilitate discussion to ensure any improvement to the process, or to the implementation can be identified and actions are taken to resolve.

All stakeholders and relevant Service Owners will be requested for information pertaining to the impact of RFC upon their operations, and will also receive a formal review report at the end of the process.

Inputs

Implemented Changes

Outputs

Review document to Change Advisory Board m Stakeholders and Service Owners
Process Improvements

Roles and responsibility

The Change Advisory Board members are responsible for appropriate review of changes and identification of improvements or additional safeguards to ensure future successful change implementation.

Closure

The formal process of RFC closure is the final step of the change Management process
The Change Advisory Board members will close all RFCs formally at the normal Change Advisory Board meeting, following any review or discussion required.

Inputs

Completed RFCs

Outputs

Closed RFCs

Roles and responsibilities

The Change Manager has the formal responsibility for RFC record closure.

Reporting

The PMU change management process incorporates several key communication opportunities.

Change Calendar

The Change Calendar will be published via the web as publicly available information. It is updated dynamically upon each visit. This allows all interested parties to see those changes which have been authorized, are still to be assessed etc.

Forward Schedule of Changes

The Forward Schedule of Changes is circulated to the Director of IT and IT Supervisory Committee where appropriate. This keeps those bodies informed of all upcoming changes.

Management Reporting

An essential element of the Change Management Process is the requirement to ensure Service Heads are well informed about all Changes relating to mission critical systems, especially those for which they have delegated accountability.

Change Process Metrics

Each step of the process should have associated metrics which allow the process quality to be monitored, and improvements to be identified.

Example metrics include:

- Time to assess
- % failed changes
- Number of assessments per RFC
- Impact as per incidents recorded

Policy 07: Data Center Operations

General Guidelines

- Staff and visitors alike may not tamper with, or in any manner adversely affect, security, infrastructure monitoring, and/or safety systems within the Data Center.
- Smoking, drinking, and eating are strictly prohibited within the Data Center raised floor space.
- Unless otherwise expressly permitted in writing, storage of combustible materials (e.g. wood, cardboard and corrugated paper, plastic or foam packing materials, flammable liquids or solvents) are prohibited within the Data Center.
- Sharing Data Center Proprietary information (like architecture, design, facilities information and services) without the express written permission is strictly prohibited.
- All hand-carry containers, boxes, bags, laptops, purses, backpacks, or equipment carried into or out of the Data Center are subject to inspection by Data Center staff and/or Security.

Physical Security

- Data Center is a secured facility. Access to the data center and other areas of the facility are restricted to persons with authorization.

- Security controls include 24 x 7 security officer presence, sign-in procedures for all ingress and egress, managed key and access card plans, managed access permissions and access request methods.
- Ingress and egress to Data Center is monitored on Closed-circuit television (CCTV) cameras
- Tampering with, or in any manner adversely affecting, security and/or safety systems within the Data Center is strictly prohibited.
- Safety and Security Departments has the right to access any part of the Data Center at any time for safety and security reasons.
- All persons entering the Data Center must:
    - Possess either authorized staff ID or authorized visitor ID
    - Have Authorization to access the facility

Rack/Cabinet and Cabling

- All refuse materials (which include, but are not limited to boxes, crates, corrugated paper, plastic, foam packing materials, and any other materials which are non-essential to the operation of equipment) must be removed. Materials must be placed in designated disposal
- All spare equipment shall be stored in a cabinet or must be kept in approved plastic or metal containers. Containers must be sealed, stacked neatly and can not impede ingress/egress or cooling.
- The tops of the cabinets or racks may not be used for physical storage.
- Mounting or hanging anything on walls of Data Center or on housed cabinets is prohibited
- “Un-racked”, operating equipment outside of cabinets/racks is strictly prohibited.
- Unsecured cabling across aisles or on the floor is prohibited. All devices must be installed in racks or cabinets.
- Cable wrapping, wire management, zip ties and/or Velcro, must be used to organize cabling in a rack or cabinet
- Cabling must not obstruct airflow / ventilation /AC (perforated tiles) or access to power strips
- All Network connected equipment is labeled with host names.

Floor Tiles

- The sub-floor (access floor) area is restricted area, accessible by or in the presence of Data Center Management Staff. The perforated tiles are strategically placed for HVAC cooling patterns in-line with the cooling requirement of the equipments/racks/cabinets

Power Protection and Backup Policy

- Main Utility Power Supply to the Data Center need upgrade should the load reaches 80% of the installed capacity
- Emergency Power Generator facility with Automatic Transfer Switch (ATS) is available to support Data Center facility for 72 minutes in absence of Utility Power Supply
- All the Distribution Communications rooms are equipped/supplied with Emergency Power in order to provide communications facility via UPS provision of power to all switches
- Power Supply to the equipment/racks/cabinets are drawn from two different panels to provide redundancy
- All the equipment housed in Data Center is properly grounded/bonded
- Sizing of the Power Protection & Power Backup device is 50% more than the projected load
- Power Backup time is greater than or equal to 90 minutes on full projected load. The system sends alert Emails/messages to the Data Center Management Staff.
- Equipment brought into the Data Center is powered in consultation with Data Center Management in order to help calculate and determine additional power draw for the new equipment being installed

Data Center Environment Policy

- Data Center temperatures are recorded/monitored and maintained in a range of 18-22 degrees Celsius
- Relative Humidity is recorded and observed in a range of 45-55%.
- Precision AC units work in rotation with at least one unit being standby at all times.
- Adequate fire detection/alarm and suppression systems are in place
- Leak detection system is in place to monitor and report on any seepages of liquids

Supplement on Disaster Recovery

Policy Statement

This functional policy covers PMU's Backup & Recovery Polices. The primary purpose for the backup system is to provide for disaster recovery of key network servers and services. The backup system is not an archival system for storing information off-line for indefinite periods of time, and is not set up to recover

individual email messages. It is each user's responsibility and obligation to ensure that all IT resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.

Each policy statement wherever required is supported by standards, procedures to achieve a complete security framework at PMU.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy statements govern the Backup & Recovery Functional Policies:

- Identify computerized systems that store information.
- Implement standard frequency of backup for each type of system or platform in use based on the significance of the information and its frequency of change.
- Implement procedures for transferring a recent copy of backup media to a physically and environmentally secure off-site storage location.
- Ensure that documented procedures exist for the recovery and restoration of information from backup media.
- Monitor backup and recovery procedures and practices to ensure compliance with this policy.
- Identify I.T. staff responsible for ensuring successful back-ups.
- Transport or provide for the transportation and storage of current backup media at an off-site storage Location.
- Ensure that a recent copy of backup media is stored off site at all times.
- Determine that the off-site storage location has sufficient physical and environmental controls to ensure the safety of backup media.

Backup & Recovery Functional Policies

Operations

- Backups are scheduled to run daily; files that were captured in weekly backup will be available for restore for a period of 3 months.

Accidental Deletion, Overwrite, Corruption

- A file that has been accidentally deleted can only be recovered from the backup system if that file existed on the network at the time of the last backup

Schedules

- Backups are to be performed, usually incremental backup daily refered as Incremental Backup.
- Schedules must be followed to perform Incremental Backup; full backup schedule should be developed to perform certain backup.
- Incremental backup will be performed request

Retention

- Depending on the type and location of the files, backup tapes are kept available for recoveries for a minimum period of 1 to 3 years before being recycled. After that, tapes should be recycled (information is overwritten) as necessary to keep the backup system running
- Off-site monthly backups to be retained for 3 years.
- Fully backed up of site is weekly, monthly and yearly, the backup media will be store in a fire proof safe off site.

Notification

- System Owners/Application owners to be notified of the status of daily backups
- Weekly status of the backup system to be notified to the Director of IT.

Recoveries

- Any file stored on a network server should be "recoverable" from tape after it has entered the backup cycle, and as long as the tape has not exceeded its retention period.
- A request for a recovery must be made to support personnel (helpdesk).
- It is not possible for individuals to recover their own files for security reasons.
- When a recovery is requested, the most recent version of a file that can be successfully recovered should be restored to the network server.
- The backup system cannot recover modifications to a file made between the last successful backup and the point of failure
- The files stored on Network Drive can be requested to be restored.

Users Responsibilities

- Users must provide support personnel with three pieces of information in order for any file to be recovered.
    - When the file was lost, deleted, overwritten, or corrupted.
    - The name (spelled correctly) of the file to be recovered
    - The full directory path to where the file was located should be passed by the user.
- Users are responsible for backing up any data not stored on Authorized Servers.

Operators Responsibilities

- Backing up systems on a daily basis /weekly basis
- Backing up all necessary data files and programs to recreate the operating environment
- Storing backup copies at an off-site location sufficiently distant from the data centre to ensure their protection if the original system is destroyed
- Backing up the printed documentation and pre-printed forms necessary for recovery
- Ensuring that backup is not continually performed on the same set of tapes
- Testing the backup to determine if data files and programs can be recovered
- Ensure that the following are stored at an off-site storage location:
    - Source and object code for production programs
    - Master files and transaction files necessary to recreate the current master files
    - System and program documentation

- Operating systems, utilities, and other environmental software

Procedures Supporting Policy

Policy 08: Security

Policy Statement

It is each user's responsibility and obligation to ensure that all resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption. This FP Intends to Clarify to all users on PMU infrastructure, what their responsibilities are; Define what the potential risks and dangers are for PMU in the event of misappropriation and abuse of Infrastructure users; and regulate the professional and effective use of Infrastructure within PMU as well as between PMU and external entities.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.

Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets

- All software assets
- All physical assets, such as computer and network equipment
- All supporting services, such as power and network link
- All of the above are either owned or leased by the PMU and under the PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy Statements govern the General Security Guidelines:

- Responsibilities for the protection of individual assets and for carrying out specific security processes must be clearly defined;
- A management authorisation process for new information processing facilities must be established;
- Advice on information security provided by in‐ house or specialist advisors must be sought and communicated throughout the organisation;
- Arrangements involving access to organisational information processing facilities by an organisation handling the outsourcing must be based on a formal contract containing all necessary security requirements;
- An inventory of all-important assets must be drawn up and maintained;
- Owners must be identified for all major assets and the responsibility for the maintenance of appropriate controls must be assigned.
- A regular inventory of assets must be performed. It's a necessary security requirements;
- Classifications and associated protective controls for information must be suited to business needs for sharing or restricting information and the business impacts associated with such needs;
- A set of operational and security procedures must be defined for information labelling and handling in accordance with the classification scheme adopted by the PMU
- An information classification scheme must be implemented

- Aspects related to information security must be addressed in an employee's terms and conditions of employment and for third parties, with a formal contract with PMU;
- Any security related incidents must be reported immediately through the established channels after the incident is discovered;
- Users of information services must be required to note and report any observed or suspected security weaknesses in or threats to systems or services;
- Mechanisms must be in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored;
- The violation of organisational security policies, functional policies and procedures by employees must be dealt with through a formal disciplinary process;
- Physical security perimeters must exist for all areas housing relevant information processing facilities;
- Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access;
- Secure areas must be created in order to protect offices, rooms and facilities having special security requirements;
- Additional controls and guidelines for working in secure areas must be used to enhance the security provided by the physical controls protecting the secure areas;
- Delivery and loading areas must be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access;
- Access to the machine rooms must be restricted to only those people who are permitted to use the machines;
- Access to the machine rooms must be monitored for illegal access attempts;

  Any information processing equipment, used for information processing on PMU's systems, but situated outside PMU's secure perimeters, must be secured in a way equivalent to PMU's on-site equipment;
- Information must be erased from equipment prior to disposal or re‐ use;
- No employee must be allowed to remove property from the PMU premises unless they have obtained authority to do so from an approving manager;
- PMU must have and implement a clear desk and a clear screen policy in order to reduce the risks of unauthorized access, loss of, and damage to information;
- Removal of any equipment, information or information facilities that belong to PMU, from the premises must be strictly monitored and controlled;
- Incident management responsibilities and procedures must be established to ensure a quick, effective and orderly response to security incidents;
- Duties and areas of responsibility must be segregated in order to reduce opportunities for unauthorized modification or misuse of information or services;

- Detection and preventive controls to protect information and information processing facilities against malicious software and appropriate user awareness procedures must be implemented;
- Back‐ up copies of essential business information and software must be taken regularly;
- Systems and applications backup documentation must include the following information:
    - Ownership;
    - Procedures;
    - System dependencies;
    - Data validation results; and
    - Source code.
- Operational staff must maintain a log of their systems operation activities;
- Faults must be reported immediately and corrective action taken;
- Regular inventory of backup media must be performed;
- The management of removable computer media, such as tapes, disks, cassettes and printed reports must be protected and controlled according to its classification;
- Media must be disposed of securely and safely when no longer required;
- Procedures for the handling and storage of information must be established in order to protect such information from unauthorized disclosure or misuse;
- Controls to prevent unauthorized access to system documentation must be developed;
- Content scanning must only be enforced in checking for malicious software, viruses or violations;
- The allocation of passwords must be controlled through a formal management process;
- A formal process must be conducted at regular intervals to review users' access rights;
- Operating systems and applications must include as a minimum, adequate user access controls, password controls and monitoring controls;
- PMU must enforce all users to follow good security practices in the selection and use of passwords;
- Users must be required to ensure that unattended equipment has appropriate protection;
- Procedures for monitoring use of information processing facilities must be established and the result of the monitoring activities reviewed regularly;
- Users must not install modems in office PC's and dial in to those PC's;
- Functional policies and procedures on the use of cryptographic controls for the protection of information must be developed and followed;
- Encryption must be applied to protect the confidentiality of sensitive or critical information;

- Digital signatures must be applied to protect the authenticity and integrity of critical electronic information, where necessary;
- Non- repudiation services must be used to resolve disputes about occurrence or non- occurrence of an event or action;
- Modifications to software packages must be discouraged and essential changes strictly controlled;
- The purchase, use and modification of software must be controlled and checked to protect against possible covert channels and Trojan code;
- Controls must be applied to secure outsourced software development.

General Security Functional

Desktop Confidentiality

- To promote desktop confidentiality the following must be adhered to:
- In an open plan office users must be aware of unauthorized users reading information displayed on their screen.
- Users must switch off their computer when it will be left unattended for an extended period of time,
- No obvious links or shortcuts to sensitive documentation must be created, e.g. shortcut for “Marketing Information.doc” on the Windows desktop.
- All Windows desktop backgrounds must be in accordance with PMU Policy
- No proprietary information must be posted on the computer screen, i.e. with post-it stickers.
- Clear Screen
- The controls pertaining to a clear screen include:

Screen Savers

A password protected screen saver will obscure the content of your computer screen after a period of no activity. Use of screen savers must be used in accordance with the following:

- User must enable screen savers on their computers, which will require input of a password if inactive for more than 15 minutes.
- Users must use screen savers, which promotes PMU business and does not offend, intimidate or disparage others.
- Users must change their screen saver password regularly,.
- Users are not allowed to disclose their screen saver password to any personnel without authorization from their direct manager at PMU.
- When entering passwords users must prevent unauthorized observation by any third party, e.g. shoulder surfing.

Computer lockout

Computer lockout must be in accordance with the following:

- Users must lock out of their workstation(s) and any active applications or log out when leaving their computers unattended.
- Users must not disclose their passwords to any personnel who want to unlock their workstation without authorization.
- A user must ensure they have logged out of all systems, including the network, after hours.

Passwords

- **Creating Passwords**: Creation of passwords must be in accordance with the following:

    - Passwords must be a minimum of six (6) characters in length for regular users, eight (8) characters in length for managers and other privileged users, and must comprise of letters, numbers, and special characters to the extent possible.
    - Passwords must not be easily associated with PMU or the user (i.e. identification number, employee number, address, numerical equivalent of name, family names, birthdate, spouse name, pet names etc.).
    - Passwords must not contain:
    - Words from a dictionary, movie or geographical location;and
    - Common character sequences such as “123456”.
    - Passwords should not be based upon month/year combinations such as "jan01" or "april2001". ‘Hackers’ use these types of words in attempts to guess passwords.
    - Users will not use cyclical passwords. For example, users cannot add a numeric at the end of the password in sequence.
    - Passwords must not consist of identical all numeric or all alphabetic characters, for example 1111111 or aaaaaaa.

- **Safeguarding Passwords:** For effective safeguarding of password, users must adhere to the following:

    - A password must be known only to the user who creates it. Passwords must not be shared with others.
    - A password must not be shared except in a temporary emergency situation. If a situation requires a password to be revealed to a second person, the owner of the password must change the

password as soon as possible after the emergency situation has passed.
    - Passwords must not be stored in readable form (i.e. writing down passwords).
    - Passwords should be changed:
    - Every 45 days or less for supervisors and other privileged users and every 90 days or less for regular users; or
    - Whenever there is any indication that the user's password has been compromised, passwords must be changed immediately.
    - As an exception, password for application user ID may be set to "never expires", provided the password is encrypted.
    - Temporary passwords assigned to users must be changed at first log-on.

- **Handling of Privileged Passwords:** Privileged passwords, such as root or super user, are powerful passwords. As such, the custodians of these passwords must properly handle them by adhering to the following:
    - A privileged password must be known only to the Administrator responsible for the system. The backup administrator should have no knowledge of it.
    - In case of emergency and in the absence of the Administrator, the backup Administrator should be given access to the password with the proper approval from his Dept. Manager. The Emergency Password form should be filled up by the requester and signed by the Dept. Manager.
    - The custodian of the privileged password must use his own account to log into the system. He should then switch from his own account to the privileged account.
    - After using the password, the backup Administrator should change the password,
    - When the Administrator returns, he should get the new password from the backup Administrator & change it.

Virus and Malicious Software Protection

- Virus Detection Programs
    - ITD should ensure that the latest version is installed on all computers.
    - Users are not allowed to remove or de-activate virus detection programs installed on their computers, without approval from ITD.

- Preventing Viruses

- Externally supplied floppy disks, CD-ROMs, and other removable storage media must not be used unless they have first been checked for viruses.
- Externally supplied computer-readable files (software programs, databases, word processing documents, spreadsheets, etc.) must be unzipped prior to being subjected to an approved virus checking process.
- If the files have been encrypted, they must be decrypted before running a virus detection program. Many virus detection programs cannot detect viruses in a zipped or encrypted file.

- Eradicating Viruses

  - Because viruses can be complex and sophisticated, users must not attempt to eradicate them without expert assistance.
  - If users suspect infection by a virus, they must immediately stop using the involved computer, disconnect from all networks, and call the Helpdesk.
  - If the suspected virus appears to be damaging information or software, users must turn the computer off immediately.

- Playing with Viruses

  Users must not intentionally write, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any PMU computer system. Such software may be called a virus, bacteria, worm, Trojan horse, etc.

- Related Functional policies

  Users must adhere to the Protection against Malicious Software and Viruses Functional Policy in particular the following:
  - Users must not open e-mail attachments from unknown sources. All e-mail attachments received from known sources must be scanned for viruses.
  - Executable attachments (i.e. .exe) must not be launched and should be deleted immediately.
  - All software and/or freeware downloaded from the Internet or attachments from mail programs used on the Internet must be scanned for viruses.

Intellectual Property Rights Protection

General

- All personal computing device software must be obtained from approved sources, as defined by PMU.
- Software not supplied by PMU or at PMU direction must not be loaded or used on PMU personal computing devices.
- Obtaining or downloading of public domain and/or evaluation copies of software from other than PMU sources is permitted only under the following conditions:
- The software must be required for a legitimate business purpose and approved by management;
- Use of the software must comply with all applicable copyright and license agreements;
- At a minimum the person obtaining the software must perform an evaluation, as to the safety and reliability of the vendor or provider of the software; and
- The software should be checked for viruses and other malicious code. This evaluation should be done on a single system before deploying the software to others.

Copyright Protection: PMU strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. Users must therefore strictly adhere to the following conditions:

- Making unauthorized copies of licensed and copyrighted software, even if only for "evaluation" purposes, is strictly forbidden.
- Reproduction of copyrighted materials may only be allowed with the permission of the author/owner or a court of competent jurisdiction.
- If users have any questions about the relevance of copyright laws, they should contact PMU IT Department.
- Unless they receive information to the contrary, users should assume that software and other materials are copyrighted.
- It is the responsibility of each employee to protect PMU interests as they perform their duties. This includes responsibility for assuring that commercial software, acquired by PMU, is used only in accordance with licensing agreements.

Back-up Protection of Information

Periodic Back-up

- All proprietary and/or valuable information resident on PMU computer systems must be periodically backed-up.
- Unless automatic back-up systems are known to be operational, all end-users are responsible for making back-up copies of sensitive, critical, or valuable files. These separate back-up copies should be made each time that a significant number of changes are saved.
- Users must ensure the back-up process was successful by restoring selected files from back-ups made.
- Access to back-up copies should be properly restricted; e.g. storage media such as disks, etc. should be locked-up and access to back-up drives should be set up with user profile access control links.

Destruction of Information

Deletion of Information

- Users are required to delete information from their computers if it is clearly no longer needed or potentially useful.
- Use of an “erase” feature (e.g. putting a document in a trash can icon) is not sufficient for proprietary information because the information may still be recoverable.
- All disks and CDs must be formatted before given to any third party or employee of PMU not authorized to see content. Users should contact the Helpdesk for assistance on formatting disk and CDs after authorization has been obtained from the owner of the information.

Destruction of Information

- Electronic Media: Prior to disposal, defective or damaged disks containing proprietary information must be destroyed using scissors or other methods approved

Asset Accountability

Information Assets

- Users must not leave proprietary information unattended e.g. at a printer or on photocopy machines.
- All users must protect information in any format (hard copy, disk, tape, etc) at the level commensurate with its classification.

Software Assets

- Users must protect personal computing device software from theft, unauthorized use, and/or unauthorized copying.
- Users are not allowed to install or remove any software from any of PMU computing equipment.

Hardware Assets

- Computing Equipment: Users' accountability for computing equipment must be in accordance with the following:
  - Users must not leave laptops unattended in an unsecured environment (on site or off-site).
  - Users must not leave laptops exposed in cars or hotel rooms.
  - User must never check-in a laptop as luggage when traveling. Always carry it on as hand luggage, in a briefcase or a laptop carry case. Airport X-ray machines do not damage data on a laptop or diskette.
  - Users must return any items issued to them (laptop computers, keys, ID cards, software, data, documentation, policys etc.) to their manager or the Human Resources (HR) Department upon resignation or termination.
  - Users are accountable for any damage to computers and related equipment in their work area.
  - Equipment and media taken off the premises should not be left unattended in public places.
  - Equipment must not be exposed to extreme heat or cold.
  - Avoid storing any devices (i.e. hard disks, etc) and equipment (i.e. laptops, desktops, etc) in automobiles.
  - Automobiles and hotel rooms are potential theft areas. Store devices out of the view of others.

Use of Networking Facilities

Use of Modems

- Modems for office computers are not permitted. Mobile and telecommuting computers are an exception to this rule. The use of modems must be approved as per the policy.
- Do not provide IP addresses or dial-up access phone numbers to vendors and/or unauthorized parties.
- Any individual who requires an individual analog line for dial-in/dial-out must obtain approval from the IT Department.

- Remote access software such as PC Anywhere or Carbon Copy is strictly prohibited from use on PMU computing resources without the expressed permission of the IT Department.
- Persons using remote, e.g., in-dial, ISDN, wireless or Internet, access to an PMU information resource must be individually identified and authenticated by an independent dedicated device such as Firewall.

Unauthorized Browsing

- Users must not browse through PMU computer systems or networks. For example, curious searching for interesting files and/or programs in the directories of other users is prohibited.
- Steps taken to legitimately locate information needed to perform one's job is not considered browsing.

Reporting and Responding to Security Incidents

Identification of Security Incidents

Methods by which suspicious activity can be identified by a user include, but is not limited to:

- Unexpected account lockout;
- Unusual last login time; and/or
- Unknown files in their file areas.

Reporting Security Incidents

- All PMU users must watch for any potential security incidents including:
    - Breaches of confidentiality;
    - Denial of service;
    - Errors resulting from incomplete or inaccurate business data; and
    - Information system failures and loss of service
- Any such incidents must be promptly reported to the Helpdesk and/or their Information Security Officers thru phone call or e-mail.
- Reporting of Weaknesses
    - Users are required to note and report any suspected security weaknesses in, or threats to, systems or services.
    - Users must not attempt to prove a suspected weakness as testing weaknesses might be interpreted as a potential misuse of the system.
- Reporting of Software Malfunctions

    - Prior to reporting software malfunctions, the following should be considered by the user:
        - The symptoms of the problem should be noted;
        - Any messages appearing on the screen should be noted;
        - Use of the computer should be suspended and the computer isolated;
        - The computer should be disconnected from PMU network; and
        - Disks, which were used on the affected computer, should not be transferred to any other computer.
- Users must not attempt to remove the suspected software, unless authorized by IT.
- Disciplinary Action
    - Users must know and understand that in the event of an incident caused by user negligence, they will face disciplinary action.
    - All users who commit security breaches will be subjected to a formal disciplinary process.

Controlling Configuration Changes on Computers

Changes to Software

PMU has a standard list of permissible software packages that users can run on their computers. Software package conditions that user must adhere to include:

- Users must not install other software packages on their computers without obtaining advance permission from IT
- Users must not permit automatic software installation routines to be run on PMU computers unless IT has first approved these routines.
- Auto discovery license management software may be used to remotely determine which software packages are resident on users' hard disks; unapproved software may be removed without giving user advance notice.
- Users are not allowed to download and install software, games and/or freeware from the Internet.

Changes to Operating System Configurations

- Users must not change their computer operating system configurations, including:
    - Upgrade existing operating systems; and/or
    - Installing new operating systems.
    - If such changes are required and authorized, they will be performed by IT

Changes to Hardware

- Computer equipment supplied by PMU must not be altered or added to in any way (e.g. upgraded processor, expanded memory, or extra circuit boards) without the prior knowledge of and authorization from IT.

Prohibited Use of Information Resources

- Any activity intended to degrade the performance of an PMU information resource, circumvent security controls, or misuse the resource in any way is prohibited.
- Users are prohibited from attempting to access other user accounts and/or files to which access has not been expressly authorized.
- All information resources, including all owned, leased and contracted services involving word processing, minicomputers, mainframes, public telephone network elements and service bureaus, must be used only as authorized by PMU
- Unauthorized use of any PMU information resource may subject the user to disciplinary action, up to and including termination of employment, termination of a supplier, contractor or agency agreement,

Protection against Social Engineering

Social engineering is the practice of impersonating someone else to gain information or services in a fraudulent manner. Employees must take steps to avoid being the victims of social engineering. Required steps include:

- Know with whom you are communicating.
- If you do not know the caller personally or suspect the caller may not be valid, insist on a callback number and before returning the call, verify that the caller is legitimate.
- You can be “spoofed” via E-mail. The name and address you receive or send to via E-mail may not be the real name and address of the person. Do not send PMU or customer proprietary information or reply with PMU or customer proprietary information to E-mail addresses you do not know or cannot verify as correct.
- Make sure that the caller has a business need to know the information they are requesting. Never furnish proprietary information until the caller's need to know has been established.

- Users who become the victim of social engineering, or social engineering attempts must report the incident to IT immediately.

PMU Internal Network Security

- When connected to and using PMU internal networks, including Local Area Networks (LANs):
    - Do not misrepresent yourself (i.e., masquerade) as someone else on the network.
    - Unauthorized individuals should not monitor network traffic (i.e., use a "sniffer" or similar device) without first obtaining explicit management approval and informing IT.
    - Do not add any network device which creates an external connection (e.g. a bridge, router, gateway, hub, modem) to your workstation without first obtaining permission from your Provider of Service.
    - Do not install file sharing or peer-to-peer software (e.g. "Napster") unless PMU provides it.
- Sharing files on your own hard drive (via network connections) can pose the following threats:
    - Unauthorized access to data files
    - Damage to data/program files - either accidental or malicious
    - Damage caused by virus attacks
- If you must allow other users to access or store files on your network connected workstation:
    - You must select either User ID access control or password access control when defining the share options for the workstation disk drives and files.
    - You must not allow ANONYMOUS FTP, TFTP, or other unauthenticated access to program or data files on your workstation.

Physical and Environmental Security

Policy Statement

This functional policy covers PMU's Physical and Environmental Security. All information, systems and assets within PMU will enforce proper and strict physical access control. Physical security measures will be implemented to ensure the physical security and integrity of building facilities and computer

centers. Protection measures will be appropriate to the classification level of the assets and information processed, stored, and handled within.

Objective

The objective of this Information Security Policies is to secure PMU Information Assets and staff. Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets (Digital Media)
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All management information systems
- All business activities supported by PMU
- All of the above are either owned or leased by the PMU and under the PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

.

Governing Policy Statements

The following Executive Policy Statements govern the Physical and Environmental Security Functional Policies listed in this document:

- Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators must be maintained;
- The risks associated with access to organisational information processing facilities by third parties must be assessed and appropriate security controls;
- All risks resulting from third party access must be reassessed on a periodic basis, or whenever such risks change;

- Arrangements involving third party access to organizational information *processing* facilities must be based on a formal contract that must contain all necessary security requirements accompanied with appropriate responsibility and confidentiality undertaking. Any violations thereto must be dealt with accordingly;
- Arrangements involving access to organisational information processing facilities by an organisation handling the outsourcing must be based on a formal contract containing all necessary security requirements.
- Physical security perimeters must exist for all areas housing relevant information processing facilities;
- ITD must ensure that secure access areas be protected by appropriate entry controls to ensure that only authorized personnel are allowed access;
- Secure areas must be created in order to protect offices, rooms and facilities having special security requirements;
- Additional controls and guidelines for working in secure areas must be used to enhance the security provided by the physical controls protecting the secure areas;
- Delivery and loading areas must be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
- Access to the machine rooms must be restricted to only those people who are permitted to use the machines;
- Access to the machine rooms must be monitored for illegal access attempts.
- Equipment must be sited and protected to reduce risks from environmental hazards and opportunities for unauthorized access;
- Equipment must be protected from power failures and electrical anomalies;
- Power and telecommunications cabling carrying data or information services must be protected from interception or damage;
- Any information processing equipment, used for information processing on PMU's systems, but situated outside PMU's secure perimeters, must be secured in a way equivalent to PMU's on-site equipment;
- All access requirements must be based on a need to know, need to do basis;
- Procedures for monitoring use of information processing facilities must be established and the result of the monitoring activities reviewed regularly.

Physical and Environmental Security Functional Policies

Access to PMU Premises

Physical Security Perimeter

- Based on a risk assessment, all PMU buildings must be classified and separated into secure areas. Based on the classification of secure areas physical security measures must be implemented to provide adequate protection.
- For all PMU facilities, a security perimeter must be established. The strength of the security perimeter will be determined by an assessment of the risks and threats to the physical environment. The security perimeter includes, but is not limited to:
    - Clearly defining the facility and security perimeter boundaries;
    - Ensuring all physical perimeter components (walls, doors, windows, etc.) are physically sound;
    - Effective access control 24 hours a day, seven days a week;
    - Implementing a manned reception area to control access to the main entry of the facility and appropriate controls to secondary entrances;
    - Implement alarmed fire control doors as per local safety requirements; and comply with all applicable safety regulations.
- Any subdivision of the PMU facilities requiring enhanced physical security must have its own physical security perimeters. These areas are referred to as “secure areas”. These areas would include, but are not limited to:
    - Computer data centres;
    - Security control centres;
    - Any vault or valuable storage facility;
    - Production or processing control centres.

Physical Entry Controls

- All PMU employees and visitors must be authorized by a PMU Head of Department/Business Unit and Security Department for physical entry into PMU facilities.
- Access rights to all areas must be reviewed on an annual basis.
- Access to areas deemed ”secure areas” (e.g. computer data centers, security control centers, valuable storage facilities or production processing centers), must be reviewed on a quarterly basis.
- Physical access to all computer rooms must be tightly controlled. Doors must be locked at all times with only authorized personnel having access.
- Authorized personnel must not allow unknown or unauthorized individuals into restricted areas without escort. Any unrecognized and unescorted personnel within a computer room must be immediately challenged to determine the reason for their presence.
- Personnel without a valid reason for being in the computer room must be escorted out of the computer room immediately and the Security

Department must be contacted through the department head or his representatives.

- It is the responsibility of each employee, vendor or visitor that has been issued an access card to immediately report lost or stolen badges.

Securing Offices, Rooms and Facilities

All Areas

All areas within PMU which need to be secured, due to the nature of the information or assets they contain, must adhere to the following controls:

- All critical computer rooms and data centres will be monitored 24 hours a day. This monitoring can be by cameras, alarmed doors and windows, people manning the centres, or a combination of the above. This monitoring ensures that unauthorized physical access to critical resources and information does not occur.
- Buildings that house the Bank's computers or communications systems must be protected with physical security measures that prevent unauthorised persons from gaining access.
- Computer room access must be limited to only those people with a valid business reason for access. Access must be reviewed quarterly and revoked immediately once it is no longer needed.
- PMU computer and data centres are restricted areas. Programmers and users are not permitted unsupervised access to the computer centres.
- Directories and internal books identifying locations of PMU information processing facilities or any other sensitive or secure area must not be readily available or accessible to the public.
- Any hazardous or combustible materials must be stored at a safe distance from any secure area per local safety regulations and manufacturer specifications.
- All doors and windows must be locked when unattended and comply with any local safety regulations.
- Rooms containing wiring or communications equipment (wiring closets, PBX rooms, etc.) must be locked at all times with access restricted to authorized personnel only. Signs are not to be posted on wiring closets, telephone rooms and other equipment components that would attract the attention of unauthorized individuals.
- Computer facility rooms must be equipped with doors that automatically close immediately after they have been opened, and which set off an audible alarm when they have been kept open beyond a certain period of time.

- To avoid unnecessary access and damages, computer facility rooms must not be used for printing, faxing, storage of computers, parts of computers or stationary.
- Computer facility rooms must not be shared with third parties.
- There must be no signs indicating the location of computer or communications centres.
- Backup and recovery media and facilities must be located at a safe distance from main facilities. The backup facilities must be at a distance that would protect it from damage from any incident at the main site.

Secure Areas

- Any person working or having access to a “secure area” must be informed of the enhanced security requirements of the “secure area”, this includes:
    - The details of the security perimeter of that area; and
    - The associated responsibilities for the area.
- Recording equipment, like photo, video, audio is not allowed unless specifically authorized by an appropriate Department/Business Unit.
- Any third party access granted to a “secure area” must be strictly controlled and monitored. All parties with access to the area must be authorized and logged. This includes support services such as cleaning or waste removal.
- Any area deemed a “secure area” must be locked when vacant and physically checked periodically. The period of checks will be determined during the designation of the security requirements for that “secure area”' and creation of the security perimeter.

Equipment Security

Cabling Security

- Ethernet ports or network cabling must not be left unprotected. Exposed Ethernet ports or cabling can be used as an entry point to the PMU network by unauthorized users.
- All power and telecommunications equipment and cabling must be protected against deliberate or accidental interruption of service. This includes protecting control boxes, cables, wiring hubs and other equipment from fire, vandalism, interception of communications or disruption of service.
- All PMU network connections must be removed and/or deactivated when a site is being vacated. Unauthorized users can use Ethernet ports or cabling that are not removed or deactivated as an entry point to the PMU network.

Equipment Maintenance

- All equipment shall be under support and/or maintenance contracts. The level of maintenance taken out is to be appropriate for the importance of the item of equipment.
- All equipment must be maintained, monitored and inspected in accordance with the suppliers' recommended service intervals and specifications to provide availability and protect the integrity and confidentiality of information.
- Only authorized maintenance personnel are allowed to perform repairs and all repairs or service work must be recorded to identify potential failure patterns.
- If equipment must be sent offsite for repairs, the confidentiality and integrity of any information must be ensured.

Equipment Staging and Protection

- The level of protection that must be provided for any information resource within PMU must be assigned and will be dependent on:
    - The criticality of the service/operation being provided by the resource. For example, Is the service provided to a single user or multiple users? Is the service critical to PMU;
    - Effect of loss on supported services/operations;
    - The monetary value of the information resource;
    - Risk of theft; and
    - Value of the resource.
- A physical location must be determined for each information resource in accordance with its specified level of protection.
- Equipment must only be sited in a physical location after due consideration of the following potential threats:
    - Theft of equipment or vandalism;
    - Vibration;
    - Impact of disasters happening in nearby premises;
    - Electrical supply interference;
    - Electromagnetic radiation; and
    - Environmental factors, such mentioned in section 3.4.
- Computer equipment must be housed in an environment equipped with fire and water detection and prevention measures.
- Rooms adjacent to the computer facility room must not be used for purposes that may involve high risks (i.e. storage space, electricity room).

- Any equipment located in publicly accessible areas, or rooms that cannot be locked, is to be fastened down by some physical means such as a cable lock system or enclosed in a lockable computer equipment unit or case.
- Clear identification of ownership should be clearly marked on all computer equipment, including the asset number.

Power Supplies

- To avoid power failures, a suitable electrical power supply must be provided in such way that Single Points of Failure can be avoided.
- Based on business criticality, the use of a back-up generator must be considered.
- Recovery procedures must be documented to ensure proper fallback or fail over processes. These procedures should be part of the disaster recovery plan.
- Uninterruptible Power Supplies (UPS) must be used for equipment supporting critical business operations to orderly close down or allow systems to continue running.
- UPS and generator equipment will be checked on a quarterly basis to ensure it has adequate capacity and tested in accordance with the manufacturer's recommendations.

Secure Disposal or Re-use of Equipment

- Any PMU information processing equipment that is to be disposed of, or reused, must undergo a cleansing process before release. The cleansing process must consist of:
    - Destruction of the information residing on equipment;
    - Validation of the process; and
    - Testing of the process to ensure no data is left on the equipment.
- If the equipment stored information classified as “confidential” or “critical” the equipment must be physically destroyed beyond repair or restoration before being disposed of.

Environmental Control

- Adequate environmental safeguards must be implemented to protect IT system resources as deemed appropriate for the sensitivity or criticality of the resource. At least the following environmental safeguards are to be assessed:
    - Fire prevention, detection, suppression and protection;
    - Water hazard prevention, detection and correction;

    - Electric power supply protection (an international guide on maximum reasonable expenditure on power protection suggests 4 percent of the value of the equipment being protected unless the mission critical nature of a particular system necessitates additional protection.);
        - Temperature control;
        - Humidity control;
        - Natural disaster protection (from lightning, etc.);
        - Magnetism protection; and
        - Good housekeeping procedures for protection against dust and dirt.
- Environmental conditions should be periodically reviewed and monitored for conditions, which could affect PMU information processing facilities.
- Fire walls surrounding computer facilities must be non-combustible and resistant to fire for at least one hour. All openings to these walls (doors, ventilation ducts, etc.) should be self-closing and likewise rated at least one hour.
- To minimize theft and water damage, multi-user computers and communications facilities must be located above the first floor in buildings.
- All computer equipment must operate in a climate-controlled atmosphere at all times. Backup ventilation plans must be provided in the event that air conditioning systems in computer rooms fail.
- Facilities management must monitor and test fire suppression system test equipment at least every 6 months and document the test results.
- All computer room personnel must be trained in the use of any automatic fire suppression systems, the use of portable fire extinguishers, and in the proper response to smoke and fire alarms.
- Use of mobile phones must be restricted inside the computer rooms.
- Fire drill for Computer Operations staff should be conducted quarterly.

Removal of Property

- Equipment, information or software should not be taken off-site without written authorization. A copy of the authorization should be kept by the user and the manager. Written authorization should include, but is not limited to the following detail:
    - The date the removal is authorized for;
    - The name of the person that granted the authorization as well as his signature;
    - The name of the person the authorization is granted to as well as his ID and signature; and
    - The serial number(s) where applicable.

- Where necessary and appropriate, equipment should be logged out and logged back in when returned (serial number(s) used, where possible).
- Spot checks should be undertaken to detect unauthorized removal of property. Individuals should be made aware that spot checks will take place.
- Computer media in transit must be protected from loss or misuse during transportation. Reliable transport or couriers should be used. Appropriate heat- resistant and water-resistant packaging should be used to protect the contents from heat, water and any physical damage likely to arise during transit, in accordance with manufacturers' specifications.

Securing Communications Networks

- Physical access to communications equipment and facilities must be restricted to authorized personnel.
- Suppliers or service engineers must be supervised when they have access to communications equipment.
- Critical areas, such as network operation centers, including those at remote sites, must be protected from power failure, such as by the use of uninterruptible power supplies (UPS).
- Communications cables should be protected by use of the following:
    - Concealed installation;
    - Armored Conduit;
    - Locked inspection/termination points;
    - Alternative feeds or routing; and
    - Avoidance of routes through public areas.
- Fiber optic cables should be used to reduce the risk of data in transit being intercepted.

Supplement on Virus Prevention, Detection, and Removal

Policy Statement

This functional policy covers PMU's Protection against Malicious Software and Viruses. Communications and operational management of information resources and systems are essential to maintaining a high level of service. Security requirements will be developed and implemented to maintain control over communications and operations
It is each user's responsibility and obligation to ensure that all IT resources are used only for its intended business purpose and that information contained or

transmitted via these resources are protected from unauthorized use, appropriation, or corruption.

Objective

The objective of this Information Security Policies is to secure PMU ’s Information Assets and staff.

Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU.

Purpose and Scope

This policy applies to ITD, Owners, their delegates and/or Custodians. In the PMU context the term “Owner” covers any of the following: an information, application, installation, network, business and/or development owner:

- All Information Assets
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All business activities supported by PMU.
- All of the above are either owned or leased by PMU and under PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy statements govern the Protection Against Malicious Software and Viruses Functional Policies listed in this document.

- Responsibilities for the protection of individual assets and for carrying out specific security processes must be clearly defined;

- The risks associated with access to organizational information processing facilities by third parties must be assessed and appropriate security controls implemented;
- Any security related incidents must be reported immediately through the established channels after the incident is discovered;
- Detection and preventive controls to protect information and information processing facilities against malicious software and appropriate user awareness procedures must be implemented;
- The management of removable computer media, such as tapes, disks, cassettes and printed reports must be protected and controlled according to its classification;
- Back‐ up copies of essential business information and software must be taken regularly;
- Content scanning must only be enforced in checking for malicious software, viruses or violations;
- Media being transported must be protected from unauthorized access, misuse or corruption;
- The purchase, use and modification of software must be controlled and checked to protect against possible covert channels and Trojan code.

Protection against Malicious Software and Viruses

Malicious Software Delivery Mechanisms

Users should also be aware that malicious software is commonly delivered by one of the following methods:

- Physical Transfer of Storage Data.
- Computer systems may become infected by exposure to a contaminated source. Malicious software can infect any form of storage media, including hard drives, diskettes, CDs, magnetic tapes and cartridges, or optical media.
- Some of the most frequent sources of contamination are:
    - Copying data from an infected diskette; and
    - Booting from an infected disk or CD.
    - Infected media may be received from another user within PMU, a vendor or even in commercial shrink-wrapped software.

Electronic Mail

- Malicious code is often spread when documents and files are sent over e-mail.

- Basic e-mail is pure text and cannot contain viruses or other malicious code.
- However, most e-mail applications today allow file attachments. These attachments may contain executable macros or scripts. When the message is received, the attached macro or script may be activated by the user, giving the malicious software an opportunity to attack and spread.

Downloaded Software

- Software downloaded from the Internet or an electronic bulletin board system may include malicious software and computer viruses.
- Files exchanged in chat sessions are becoming a frequent method of propagating malicious software.

Mobile Code

- Mobile code is software that will run on multiple platforms.
- Mobile code is contained in small applications called applets, which are often used on Web pages to provide news tickers; front-end graphical user interfaces (GUIs) and video games.
- Some examples of programming languages used in developing mobile code include Java, JavaScript, ActiveX, and Postscript.
- Malicious code can be hidden within Java applets, ActiveX controls and plug-ins to steal information from a computer file or disable a system.

Preventing Malicious Software and Viruses

To protect PMU resources against the risk of physically transferred malicious code, the following protection measures must be adhered to:

Physical Transfer

- Users should avoid booting or copying files from removable media such as USB drives or CD-ROM's unless they have been obtained from a trusted source.
- Users should avoid leaving removable media such as diskettes and CD-ROM's in boot-able drives.

- All storage media obtained from sources external to PMU must be scanned by an approved anti-virus software product with current signature files prior to use.
- Prior to providing storage media to customers, vendors, or others outside PMU, the media must be scanned by an approved anti-virus software product with current signature files.

Electronic Mail

- Users should be suspicious of all e-mail messages from people that they don't know.
- All e-mail messages that include attachments should be viewed with suspicion. Users should know the purpose of attachments before opening them.
- Suspicious e-mail messages with executable attachments (e.g. com or exe) should not be opened, even if they appear to be from people known to the user (s).
- Macro programs contained in Word or Excel files received by e-mail should not be executed until it has been determined that they are from a trusted source.

Downloaded Software

- Software should not be downloaded from an unknown or un-trusted source.
- Obtaining or downloading of public domain, shareware, or evaluation copies of software from other than PMU sources is permitted only under certain conditions.
- Software downloaded from sources external to PMU must be scanned by an approved anti-virus software product with current signature files prior to being installed on an PMU information resource.

Mobile Code

- In an interactive environment, a server is accessed across a network and an application (applet) is downloaded onto the computer that is then executed. The Users web browsers should be configured to prevent downloading of applets.
- Java and ActiveX should only be enabled when they are needed to access a trusted Web site.

Application Software

- Many software applications such as Internet Explorer, Mozilla Firefox and Google Chrome and the Microsoft Office Suite, contain features designed to alert the user before opening or activating files that could contain potentially dangerous software.
- Users should carefully consider the source of files that are flagged in this manner.
- Users should not configure the application software to disable these warnings.

Anti-Virus Software

Anti-Virus software is the main line of defense against computer viruses.

ITD responsibilities include:

- Ensuring that current, University approved, anti-virus software is installed and activated on all computers issued to users.
- Configuration of the software to scan all file types, not just executables.

User responsibilities include:

- Software must not be written; generated, copied, propagated or executed that will damage or hinder the performance of any PMU information resource.
- Users of any PMU PC must ensure that current; University approved, anti-virus software is activated on their PC. This software must be actively enabled at all times.

Detecting Malicious Software and Viruses

Identification of Malicious Software

- Malicious software can be identified through observation, technical knowledge, or virus alerts.
- Several factors can indicate that malicious code has infected a system. Below are some indicators to help confirm the presence of a virus:
- File size increase;
- Change in update timestamp;
- Sudden decrease of free space;
- Numerous unexpected disk accesses; and

- Strange macros attached to files.

Further Guidelines

- The anti-virus software should be used to perform a periodic scan of all files on the system. PMU ITD maintains a local signature server that contains the most recent updates. All University laptops and Desktops are configured to get their updates from this central server.
- Any machine suspected to be infected by a virus is immediately disconnected from all networks. The machine must not be reconnected to the network until IT staff can verify that the virus has been removed.

Reporting Malicious Software and Viruses

- Malicious software can spread quickly and needs to be eradicated as soon as possible to limit damage to PMU information resources.
- Reporting actual attacks by viruses or other malicious software is important because it allows PMU to collect information regarding the magnitude and severity of the attack and to take appropriate steps to halt further contamination.
- For assistance in removing a virus or other malicious software, if needed, or for help repairing any damage that resulted, users should contact the Help desk.
- Any significant malicious software attacks must be reported to the Help desk for further investigation and assessment. An attack should be considered "significant" if one or more of the following apply:
  - The infection has caused the loss or damage of PMU data;
  - The infection has impacted more than one computer or system; and/or
  - The infection is the result of a virus that has previously been assessed by PMU as a high risk.
- Correcting Malicious Software and Viruses
- Backup
  - The ability to recover from a malicious attack depends upon maintaining frequent backups.
- Recovery
  - If it is not practical or feasible to obtain a new copy of the file without the virus, when attempting recovery, anti-virus software may be used to remove the virus.
- Virus Hoaxes

- A virus hoax is the fraudulent report of a virus for the purpose of generating large amounts of network traffic about the non-existent virus.
- While PMU will sometimes make use of established employee communications channels to distribute information regarding viruses, users must ignore and not forward e-mail or other messages originating from other sources regarding supposed viruses.
- Passing on messages about hoaxes only serves to further propagate them and unnecessarily increase the utilization of PMU resources.
- PMU security personnel regularly receive information from the major anti-virus software vendors and other sources. It is not necessary to pass information to them regarding possible viruses

Supplement on SPAM, Intrusion Prevention and Detection

Policy Statement

It is each user's responsibility and obligation to ensure that all resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption. This FP Intends to Clarify to all users on PMU infrastructure, what their responsibilities are; Define what the potential risks and dangers are for PMU in the event of misappropriation and abuse of Infrastructure users; and regulate the professional and effective use of Infrastructure within PMU as well as between PMU and external entities.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff. Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets (Digital Media)
- All software assets

- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All management information systems
- All business activities supported by PMU.
- All of the above are either owned or leased by the PMU and under the PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy statements govern the Combating Cyber Crime Functional

Policies listed in this document:

- Intrusion detection software which records attempted and successful access to your systems.
- Access control lists and facilities, which record certain activities for specific files, such as: read, write, execute, and delete
- Network usage analysis, which identifies application access and reports on user authorization levels
- Network packet sniffing software to detect attack origins
- Disable specific applications, for example, an e-mail system subjected to a SPAM attack
- Ensure that all system and access events are logged
- Gather evidence to prove malicious intent, especially if the suspects are organization staff
- Access Controls should limit access to only those persons so authorized. Use a combination of policies and guidelines to promote both awareness and compliance
- Implement strong authentication and appropriate access control measures.
- Always perform rigorous System Testing before releasing into live 'production'
- Restrict and control all software and utilities which could be used inappropriately

- All software downloads must be virus-scanned
- Deploy software scanning tools to detect the 'footprint' of malicious code, introduced via e-mail, Internet download or by other means, e.g. diskette or CD-ROM
- Foster a sense of constant vigilance throughout the organization
- Nominate a technically oriented member of staff as 'virus control officer' to be the first point of contact for all virus alert issues and who co-ordinates follow up actions
- Advise staff of virus reports identified as hoaxes, in order to minimize disruption to business
- Considering designating a specific telephone extension as the virus 'hotline', reserved for virus and other malicious code reports / warnings.
- The Information Security Officer, the System Administrator, and the nominated virus control officer should collaborate to prepare a **Virus Incident**

Response Plan

- Ensure that **all** PCs are protected, and that regular anti-virus updates are distributed
- After a virus attack, consider regularly reviewing software and files used for critical business processes to identify and investigate unauthorized and / or suspicious changes
- Promote awareness of the risks and encourage best practice regarding the receipt of e-mail attachments
- Consider the optimum deployment: servers only, or servers and workstations. The latter is recommended
- Ensuring that the license agreement includes updates of the anti-virus software and of the vaccine files
- Choosing e a vendor who offers 'hotline' support to deal with newly released virus strains

Functional Policy

Combating Cyber Crime

Cyber Crime remains a major area of Information Security risk. The sophistication of these threats is consistently increasing and the methods employed to combat these threats must match this level of sophistication. As a result, it is necessary for all systems users to be especially vigilant at all times

Defending Against Premeditated Third Party Cyber Crime Attacks.

Criminals may target organization's information systems, resulting in serious financial loss and embarrassment.

- Security on the network is to be maintained at the highest level. Those responsible for the network and external communications are to receive proper training in risk assessment and how to build secure systems which minimize the threats from cybercrime.

Minimize the Impact of Cyber Attacks.

Even the most Information Security conscious organizations can be attacked; this may be to 'prove a point' or for other malicious reasons

- Plans are to be prepared, maintained and regularly tested to ensure that damage done by possible external cybercrime attacks can be minimized and that restoration takes place as quickly as possible

Collecting Evidence for Cyber Crime Prosecution

In order to prosecute Cyber Crime successfully you need proof. This can be difficult to provide, unless your organization's information systems have adequate controls and audit capabilities.

- Perpetrators of cyber-crime will be prosecuted by PMU . Suitable procedures are to be developed to ensure the appropriate collection and protection of evidence

Defending Against Premeditated Internal Attacks

Access to confidential data may be legitimized in employees' job descriptions. The act of copying sensitive data may not necessarily leave a 'footprint' on the system, and such copies can then be exported from your organization by e-mail or by removable media without leaving a trace. The effects of outright malicious data destruction are obvious, but the computer entry process of so doing may have seemed routine.

- To reduce the incidence and possibility of internal attacks, access control standards and data classification standards are to be periodically reviewed whilst maintained at all times

.

Defending Against Opportunistic Cyber Crime Attacks

Opportunistic criminal attacks usually arise from chance discovery of a loophole in the system, which permits access to unauthorized information

- It is a priority to minimize the opportunities for cyber crime attacks on PMU systems and information through a combination of technical access controls and robust procedures

Safeguarding against Malicious Denial of Service Attack.

Denial of Service (DoS) attacks have gained notoriety as being an effective way to disable Web based services. See DoS for an explanation of the techniques used and their consequences.

- Contingency plans for a denial of service attack are to be maintained and periodically tested to ensure adequacy

Defending Against Hackers

Unlike other forms of Cyber Crime, these attacks take a 'scatter gun' approach, in that they do not target a specific organization. If you happen to be 'in the firing line', and your Information Security safeguards are poor, you are likely to be hit.

- Threats to PMU-IT systems and information are to be minimized by fostering staff awareness, encouraging staff vigilance, and deploying appropriate protective systems and devices

Handling Hoax Virus Warnings

Threats from viruses are well known throughout the IT community. Hoax threats - the spreading of rumors of fictitious viruses or other malicious code - can waste time, as staff attempt to locate a virus which does not exist

Vigilance and good virus intelligence warnings are the key to minimizing the impact of hoaxes.

Defending Against Virus Attacks

Virus infection can be minimized by deploying proven anti-virus software and regularly updating the associated vaccine files. Many anti-virus companies supply such updates from their Web sites.

- Without exception, Anti Virus software is to be deployed across all PCs with regular virus definition updates and scanning across both servers, PCs and laptop computers

Responding to Virus Incidents

Despite general awareness and technical safeguards, some viruses nevertheless enter and infect the organization’s systems. Dealing with a virus in a professional

and planned way reduces both its impact and its spread throughout the organization and beyond.

- The threat posed by the infiltration of a virus is high, as is the risk to PMU - IT systems and data files, Formal procedures for responding to a virus incident are to be developed, tested and implemented.
- *Virus incident response must be regularly reviewed and tested*

Virus Scanning Software

The development of anti-virus software is a highly technical and specialized area. Consequently, selection of the product should be with utmost care.

- Anti Virus software must be chosen from a proven leading supplier

Supplement on Authentication and Passwords

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.

Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets (Digital Media)
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All management information systems
- All business activities supported by PMU.
- All of the above are either owned or leased by the PMU and under the PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy,

and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy Statements govern the Functional Policies on Log on and Authentication listed in this document:

- Business requirements for access control must be defined and documented, and access must be restricted to what is defined in the access control policy.
- All access requirements must be based on a need to know, need to do basis.
- The allocation of passwords must be controlled through a formal management process.
- Operating systems and applications must include as a minimum, adequate user access controls, password controls and monitoring controls.
- Each System Owner at PMU must enforce all users to follow good security practices in the selection and use of passwords.
- Access by remote users must be subject to authentication.
- Connections to remote computer systems must be authenticated.
- The procedure for logging onto computer systems must be designed to minimize the opportunity for unauthorized access.
- User identification and authentication must be strictly enforced.
- Access to information services must use a secure log‐ on process.
- All users must have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual.
- A password management system must be in place to provide an effective, interactive facility that ensures quality passwords.
- Use of system utility programs must be restricted and tightly controlled.
- Inactive terminals in high risk locations or serving high risk systems must shut down after a defined period of inactivity to prevent access by unauthorized persons.
- Restrictions on connection times must be used to provide additional security for high‐ risk applications.
- Audit logs recording exceptions and other security‐ relevant events must be produced and kept for an agreed period to assist in future investigations and access control monitoring.
- Procedures for monitoring use of information processing facilities must be established and the result of the monitoring activities reviewed regularly.
- Computer clocks must be synchronized for accurate recording.

Authentication Functional Policies

- Log on
    - Pre-Log on Banner: All computer systems within PMU must contain a pre-log on warning banner to address the following:
        - Before being given the opportunity to log onto a computer facility, intended users will be presented with a login banner, where applicable.
        - This provides: Users with a chance to terminate the login before accessing a computer that they are not authorized to; Identification of PMU, the network, location, or host must not appear prior to a successful login.
        - Systems must be configured to not give any information on an unsuccessful login. This includes identifying which portion of login sequence (user ID or password) was incorrect.

- Authentication
    - User Identification
        - All users must have their identity verified with a user ID and a secret password, or by other means that provide equal or greater security, prior to being permitted to use PMU information resources.
        - Unless prior permission from the ITD has been granted, all System Administrators must consistently observe the user-ID naming standards.
        - Each computer and communication system user-ID must be unique and forever connected solely with the user to whom it has been assigned.
        - After a worker leaves PMU, there should be no re-use of any user-IDs. Any exceptions should be authorized. This serves to minimize the risk of dormant access permissions being inherited by a new user.
        - Administrators with access to super user or privileged accounts must use their account to log into systems. They should then switch from their own accounts to the privileged account.

    All Guest Accounts must be disabled on servers, desktops, databases and applications.

Assigning Passwords

Administrator's responsibilities when assigning passwords include:

- The initial temporary password assigned to users must be a minimum of six (6) characters in length and comprised of alphanumeric, non-alphanumeric and special characters.
    - Passwords assigned must be unique for each user.
    - Passwords must only be supplied to users in a secure manner e.g. not via a third party.
    - Initial passwords must not be easily associated with PMU or the user (i.e. identification number, employee number, address, numerical equivalent of name, etc.)
    - On initial log on, new users will be forced by the system they are accessing to change their initial password to one that meets the relevant password functional policies.

Safeguarding Passwords

Administrators must adhere to the following regarding safeguarding of passwords:

- ITD must perform password testing on quarterly basis to ensure proper passwords are being used. This includes the use of password cracking tools.
- This process must be controlled in the strictest manner and subject to explicit supervision.
- Users whose password is cracked must be notified immediately, their account disabled, and a new password issued using the normal allocation methods.
- Users must be forced to change passwords every Academic semester. System administrators shall enforce this through technical means by deploying password aging on systems.
- Default passwords shipped with servers, operating systems software or applications must always be changed when the hardware or application is installed or implemented.
- Where technically feasible, systems must use password history techniques to maintain a password history of users. This will ensure that users do not reuse passwords when forced to change the password.
- All computers, databases or applications that store user account and password information must be secured in the strictest manner. Access to the user account base must be restricted to only authorize administrators.
- This access must be reviewed at least twice a year along with a technical review of the host/server/user store.

System Account Controls

General Account Controls

General account controls include the following:

- For high security environments it may be necessary to limit session initiation to specific terminals or locations. In this case, unique device identifiers must be associated with the approved connection points or direct connection to a server may be required.
- Users given command line access to systems must, where feasible, be limited to the access or service needed. This may include restricted shells, application menu restrictions, and the like.
- Unless authorized to the user, systems should not allow users to have multiple sessions on the same system.

Account Lockout

- Upon three consecutive authentication failures, users must be locked out of the resource in which they are attempting to gain access to and will have to have their account policy reset.
- In the event that an account requires a new password, Help desk/System Administrator personnel must be contacted.
- In the event that the account requires resetting without changing the password, the reset must only be executed after verification of the user's identity.

Disabling Inactive Accounts

User accounts that have not been accessed for 90 days must automatically be disabled.

Automatic time-outs

Automatic time-outs must be in accordance with the following:

- PC's/laptops and Servers, when applicable, must be configured with a password-protected screen saver. The screen saver must require the entry of a password after a PC/laptop or Server console has been left idle for five (15) minutes.
- Systems must force users off after 30 minutes of inactivity. The user should have to log back into the system.

- System sessions that are not active for two (2) hours will be automatically terminated. For those systems that cannot automatically terminate connections, password protected screen savers or terminal locks must be activated.

Use of System Utilities

A number of utilities are available to enable system administrators to perform low-level maintenance tasks on a system. If inappropriate access is gained to these utilities they may be used to circumvent logical security controls. All utilities must:

- Be stored off-line if not required on a daily basis;
- Have access restricted to a very limited group of authorized users; and
- Include logging facilities to record their use.

Application Access Controls

All users must only be provided with the minimum level of access required to perform their duties. This should be achieved using a combination of:

- Logical security within an application;
- Hiding the availability of unauthorized options;
- Limiting file permissions, e.g. read-only- Control of output distribution.

Monitoring System Access and Use

For applications that will be initiated and developed from the publication date of this document, the application program should pass the user logon ID to the Oracle database for proper monitoring.

Clock Synchronization

System clocks must be synchronized to an agreed standard to ensure the accuracy of audit logs. For example, Greenwich Mean Time or Local time.

System Monitoring

System Administrators must ensure that monitoring tools are installed in order to log user access activity and security violations against critical production data.

Security Event Logs

- Computer and communications systems handling sensitive, valuable, or critical PMU information must securely log all security relevant events.

- Logs containing computer or communications system security relevant events must be retained for a period prescribed. During this period, logs must be secured such that they cannot be modified, and such that they can be read only by authorized persons.
- ITD will review records reflecting security relevant events in conjunction with Computer Operations and Systems Administration staff. All potential security incidents must be reported immediately.
- Security Administrator must ensure that monitoring tools are installed in order to log user access activity and security violations against critical production data.

Supplement on Incident Handling and Reporting

Policy Statement

This functional policy covers PMU's Incident Handling and Reporting. In order to minimize the damage from security incidents and malfunctions within PMU, adequate security controls will be followed and security will be monitored to detect security breaches, incidents or areas of non-compliance with security policies, Functional Policies and procedures.

It is each user's responsibility and obligation to ensure that all IT resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.

Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets (Digital Media)
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link

- All management information systems
- All business activities supported by PMU.
- All of the above are either owned or leased by the PMU and under the PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy statements govern the Incident Handling and Reporting Functional Policies listed in this document:

- Training and orientation are provided to newly hired employees through the induction process;
- Any security related incidents must be reported immediately through the established channels after the incident is discovered;
- Procedures must be established and followed for reporting software malfunctions;
- Users of information services are required to note and report any observed or suspected security weaknesses in or threats to systems or services;
- Mechanisms must be in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored;
- The violation of organisational policies, functional policies and procedures by employees must be dealt with through a formal disciplinary process;
- Incident management responsibilities and procedures are established to ensure a quick, effective and orderly response to incidents;
- Faults must be reported immediately and corrective action taken;
- An intrusion detection system is in place to detect unauthorized use of PMU networks;
- Audit logs recording exceptions and other security‐ relevant events are produced and kept for 3 months to assist in future investigations and access control monitoring.

Incident Handling and Reporting

Incident Levels

All incidents must be reported based on the severity of the incident and can be classified as one of the following:

Critical Alert

A critical alert is an event that is, or could become a serious and immediate threat to any of the devices on PMU network and requires immediate attention and action.
Threatened devices may include routers, networks, servers, firewalls, network management hosts, attached LAN's, or user hosts.

Major Alert

A major alert is an event that is, or could become, a future threat, but which has not been
determined as serious enough as of that time. Hence, it may or may not require an immediate response depending on the incident.

Minor Alert

A minor alert is an event that is, or could become, a minor annoyance or threat; or which has been determined to be a non-threat resulting from either authorized, or unauthorized network activity.

Minor alerts are informational in nature.

Types of Incidents

The type of incidents which can be reported by users, include but is not limited to the following:

- Accidental and/or negligent incidents, including:
- Compromise of system integrity;
- Denial of system resources;
- Illegal access to a system (either a penetration or an intrusion);
- Malicious use of system resources,
- Any kind of damage to a system.
- Power Outages

Reporting Security Incidents

Reporting Violations

- All incidents will be reported to the IT Help Desk
- Help Desk will escalate the incident for investigation to appropriate senior personnel.
- All incidents will be investigated by ITD to determine the severity of the incident.
- Investigative methods and procedures will be used based upon the Security Incident Level.
- In cases where the violation is clearly illegal with intent, notification to the Higher Management shall be immediate.
- In cases where the intent is not clear, the violator shall be advised to correct the violation. A repeat violation shall be reported immediately to management and the appropriate disciplinary action will be taken based on the severity of the incident.
- In cases where the violation is either a support or resource-sharing issue, the violator will be informed of the violation and advised of possible corrective action. Records shall be kept of such violations.
- If support teams determine that repeated violations of policies and functional policies are causing support or resource-sharing problems, they may contact ITD who may defer support and/or report the violation to ITD management.
- No PMU employees are allowed to talk about any security incident in public or media.

Responding to Incidents

ITD Responsibilities

The ITD have the following responsibilities when responding to incidents:

- Confirming that an intrusion has occurred (or is occurring).
- Keeping records of work efforts.
- Activating additional event logs immediately.

Initial Analysis

- To be able to address incidents properly it might be necessary to collect evidence as soon as possible after the occurrence.
- Regardless of how the suspicious activity is identified, the administrator must quickly perform an initial analysis to determine if the possible intrusion is the result of:
    - Hardware or software problems;

    - User error; or
    - An actual security intrusion.
- The initial analysis must be performed immediately, so that innocent activities can be quickly eliminated, and intrusions can get prompt attention.

Taking Action

- If PMU information resources are in danger of being irreparably harmed, the administrator of the system must take immediate action to protect these resources.
- Examples of irreparable harm include, but are not limited to:
    - An intruder has entered a system and is in the process of destroying or damaging data that cannot be recovered;
    - An intruder is actively bringing systems down and impacting customer service; or
    - An intruder is actively engaged in other behavior that will cause unrecoverable loss or damage to PMU or PMU information resources.
- Examples of protective actions to be taken could include, but are not limited to:
    - Disabling all system accounts and/or changing all system passwords and/or disabling access permissions;
    - Correcting the vulnerability that allowed the intruder to gain access in the first place;
    - Removing or shutting down the access method being used by the intruder;
    - Bringing the system down or disconnecting it from the network; and
    - Physically removing disk drives, tape files, or other system resources.
- Where feasible, any action taken should be performed in a manner to prevent the intruder from being made aware that his actions have been noticed.
- Security violations will be followed by corrective action by management and the users involved in the incident.

Learning from Incidents

- All security violations and other incidents investigated must provide sufficient information so that management can take steps to ensure that:
    - Such incidents cannot reasonably take place again; and
    - Effective security measures have been re-established.
- Information that should be collected by the investigating body during the investigation, include:

    - Time spent on incident;
    - The type of incident; and
    - Cost of incident or malfunction. Loss due to man-hours must be calculated for all incidents.
- Summary reports of all incidents should be maintained by ITD for historical documentation.

Disciplinary Action

- Users must know and understand that in the event of an incident caused by user negligence, they may face disciplinary action.
- Disciplinary actions must be co-ordinate by the ITD through the Human Resource (HR) Department.
- All users who commit security breaches may be subjected to a formal disciplinary process.